FLUKE networks

AirCheck™

Wi-Fi Tester

Bedienungshandbuch

January 2010, Rev. 2 4/11 (German)
©2010-2011 Fluke Corporation. All rights reserved.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the WiFi Alliance.

BESCHRÄNKTE GARANTIE UND HAFTUNGSBEGRENZUNG

Fluke Networks gewährleistet, dass jedes Produkt unter normaler Nutzung und normalem Service frei von Material- und Fertigungsdefekten ist. Die Garantiedauer für das Hauptgerät beträgt ein Jahr und beginnt mit dem Kaufdatum. Für Einzelteile, Zubehör, Reparatur- und Wartungsarbeiten wird, sofern nicht anders festgelegt, eine Garantie von 90 Tagen übernommen. NiCd-, NiMH- und Lithium-Ionen-Akkus, Kabel oder andere Peripherieprodukte gelten als Einzelteile oder Zubehör. Die Garantie erstreckt sich ausschließlich auf den erstmaligen Käufer bzw. Endbenutzer eines von Fluke Networks autorisierten Einzelhändlers und gilt nicht für andere Produkte, die nach Ermessen von Fluke Networks unsachgemäß verwendet, verändert, vernachlässigt, verunreinigt, durch Unfälle beschädigt oder abnormalen Betriebsbedingungen oder einer unsachgemäßen Handhabung ausgesetzt wurden. Fluke Networks gewährleistet, dass die Software für 90 Tage dem Wesen nach gemäß den Funktionsbeschreibungen funktioniert und auf einem nicht defekten Datenträger aufgezeichnet wurde. Fluke Networks gewährleistet nicht, dass Software fehlerfrei ist oder unterbrechungsfrei betrieben werden kann.

Von Fluke Networks autorisierte Einzelhändler dürfen diese Garantie nur auf neue und nicht gebrauchte Produkte für Endbenutzerkunden ausdehnen, haben jedoch keine Befugnis zur Erteilung einer umfassenderen bzw. anderen Garantie im Namen von Fluke Networks. Garantieunterstützung ist nur verfügbar, wenn das Produkt über eine von Fluke Networks autorisierte Verkaufsstelle gekauft wurde, bzw. der Käufer den geltenden internationalen Preis bezahlt hat. Fluke Networks behält sich das Recht vor, Käufern Importkosten von Reparatur-/Ersatzteilen in Rechnung zu stellen, wenn das in einem Land gekaufte Produkt in einem anderen Land zur Reparatur eingereicht wird.

Die Garantieverpflichtung von Fluke Networks ist, nach Ermessen von Fluke Networks, auf Rückerstattung des Kaufpreises bzw. Ersatz eines defekten Produkts beschränkt, das innerhalb der Garantiedauer an ein von Fluke Networks autorisiertes Servicezentrum zurückgesendet wird.

Um Garantieleistung in Anspruch zu nehmen, wenden Sie sich für Rücknahmeinformationen an das nächstgelegene von Fluke Networks autorisierte Servicezentrum, und senden Sie dann das Produkt mit einer Beschreibung des Problems vorfrankiert und versichert (Frachtfrei-Bestimmungsort) an dieses Servicezentrum. Fluke Networks übernimmt keine Haftung für Beschädigungen während des Transports. Nach Reparatur innerhalb der Garantiedauer wird das Produkt unter Vorausbezahlung der Transportkosten (Frachtfrei-Bestimmungsort) an den Käufer zurückgesendet. Wenn Fluke bestimmt, dass der Defekt auf unsachgemäße Verwendung, Veränderung, Fahrlässigkeit, Unfälle oder abnormale Betriebsbedingungen oder unsachgemäße Handhabung oder normale Abnutzung bzw. Verschleiß mechanischer Teile zurückgeführt werden kann, wird Fluke Networks dem Käufer einen Voranschlag der Reparaturkosten zustellen und vor Beginn der Reparatur die Zustimmung des Käufers abwarten. Nach Reparatur wird das Produkt unter Vorausbezahlung der Transportkosten an den Käufer zurückgesendet, und dem Käufer werden die Reparaturkosten und die Rücksendungskosten (Frachtfrei-Versandstelle) in Rechnung gestellt.

DIESE GARANTIE STELLT DEN EINZIGEN UND ALLEINIGEN RECHTSANSPRUCH AUF SCHADENERSATZ DES KÄUFERS DAR UND GILT AUSSCHLIESSLICH UND AN STELLE ALLER ANDEREN VERTRAGLICHEN ODER GESETZLICHEN GEWÄHRLEISTUNGSPFLICHTEN, EINSCHLIESSLICH - JEDOCH NICHT DARAUF BESCHRÄNKT - DER GESETZLICHEN GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT UND DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. FLUKE NETWORKS HAFTET NICHT FÜR SPEZIELLE, UNMITTELBARE, NEBEN- ODER FOLGESCHÄDEN ODER VERLUSTE, EINSCHLIESSLICH VERLUST VON DATEN, UNABHÄNGIG VON DER URSACHE ODER THEORIE.

Da einige Länder oder Staaten eine Einschränkung der gesetzlichen Gewährleistung oder den Ausschluss oder die Beschränkung von Neben- oder Folgeschäden nicht zulassen, gelten diese Einschränkungen und Ausschlüsse möglicherweise nicht für alle Käufer. Sollte eine Klausel dieser Garantiebestimmungen von einem zuständigen Gericht oder einer anderen Entscheidungsinstanz für unwirksam oder nicht durchsetzbar befunden werden, so bleibt die Wirksamkeit oder Durchsetzbarkeit anderer Klauseln davon unberührt.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Inhalt

Titel **Seite**

Einführung 1
Registrieren des Produkts 1
Fluke Networks-Wissensdatenbank 1
Kontaktaufnahme mit Fluke Networks 2
Sicherheitsinformationen 2
Auspacken 3
    AirCheck Wi-Fi Tester 3
    AirCheck Frontline-Fehlerbehebungs-Kit 3
Äußere Merkmale 4
Laden und Betriebsdauer des Akkus 6
Mindestkonfiguration für bestmögliche Leistung 7
Informationen über Netzwerke 8
    Was befindet sich im WLAN? 8
    Können Geräte eine Verbindung zum Netzwerk herstellen? 9
    Was ist der Grund für schwache Netzwerkleistung oder Verbindungsverluste? 10
    Weist das Netzwerk Sicherheitsrisiken auf? 11
    Welche Netzwerke oder Access Points kommen bei Bewegung in Reichweite? 12
    Wie kann ich mein Netzwerk und meine Testsitzung dokumentieren? 12
    Wo befindet sich ein Access Point? 12

HOME-Bildschirm (Startbildschirm) 13
Tester einrichten 14
    Ändern der Sprach- und Landeseinstellungen 14
    Erstellen eines Profils für Verbindungen zu gesicherten Netzwerken 14
    Einstellungen 16
    802.11d-Betrieb 20
    Ändern der Schwellenwerte für die Farben in Balkendiagrammen 21
    Zuordnen eines Autorisierungsstatus zu Access Points 22
Erkennen von Netzwerken und Access Points 23
Wenn der Tester keinen Access Point erkennt 34
Notizen für Netzwerke und Access Points 35
Kanalauslastung 38
Verbindungsprüfung 41
    Laden eines Profils, das Sicherheitsanmeldeinformationen einschließt 42
    Herstellen einer Verbindung mit einem Netzwerk oder Access Point 42
    Pingen eines Geräts oder Webservers 46
Ermitteln von Clients 49
Wenn der Tester keinen Client erkennt 54
Einen Access Point oder Client lokalisieren 54
Der externen Richtantenne 58
Signalstärkemessungen so einstellen, dass sie mit anderen Geräten übereinstimmen 61
Speichern einer Testsitzung 62
Verwalten von Dateien auf dem Tester 63
    Dateien auf dem Tester 64
    Transferieren von Dateien auf einen PC 65
Wartung 65
    Reinigen des Testers 66
    Aktualisieren der Software im Tester 66

Werkseitige Standardeinstellungen wiederherstellen 67
Gerätinformationen 67
Wenn der Tester nicht ausschaltet 67
Optionen und Zubehör 68
Spezifikationen 69
Umweltspezifikationen 69
Allgemeine Spezifikationen 71
Wireless-Spezifikationen 72
Erklärung zu Störaussendungen – FCC (Federal Communication Commission) und IC (Industry Canada) 75
Wichtiger Hinweis: Erklärung zur Strahlenbelastung – FCC und IC 75
Europa-EU Konformitätserklärung 76
Anhang A: Protokollmeldungen für fehlgeschlagene Verbindungen 79
Anhang B: Standardeinstellungen 83
Anhang C: 802.11d-Ländercodes 85
Index 95

Abbildungen

Abbildung		Seite
1.	Äußere Merkmale	4
2.	Entfernen der Batterie	6
3.	HOME-Bildschirm (Startbildschirm)	13
4.	Ändern der Schwellenwerte für die Farben in einem Balkendiagramm	21
5.	Netzwerke (**SSID**s)	24
6.	Access Points-Liste	28
7.	Access Point-Details	32
8.	Kanalverwendung/Kanalauslastung	39
9.	Details zur Kanalverwendung/Kanalauslastung	40
10.	Der Verbindungsbildschirm	44
11.	Verbindungsprotokoll	45
12.	Ping-Bildschirm	47
13.	Clients-Bildschirm	50
14.	Bildschirm zu Client-Details	52
15.	Lokalisieren des AP	55
16.	Bildschirm „Client lokalisieren“	56
17.	Suchmuster für die Rundstrahlantenne im Tester	57
18.	Suchmuster für die externe Antenne	59
19.	Richten der externen Antenne	60
20.	Antennenmuster für die externe Antenne (Magnitude (dBi)) vs. Azimut (Grad)	74

AirCheck™ Wi-Fi Tester

Einführung

Mit dem AirCheck™ Wi-Fi Tester können Sie sicherstellen, dass 802.11 Wireless-LANs (WLAN) für mobile Benutzer verfügbar sind, und die Auslastung der Kanäle untersuchen, um eine Analyse des Netzwerkzustands durchzuführen und die Quelle von Verbindungsproblemen zu finden. Der Tester funktioniert in 802.11 b/g/n-Netzwerken in 2,4-GHz-Band und 802.11 a/n-Netzwerken im 5-GHz-Band.

Der optionale PoE-Detektor (PoE = Power over Ethernet) zeigt an, wenn PoE-Spannung von 802.3af-Geräten und Hochleistungs-802.3at-Geräten auf Twisted-Pair-Netzwerkverkabelung verfügbar ist.

Die Testergebnisse können gespeichert werden. Mit der AirCheck™ Manager-Software können die Ergebnisse auf einen PC übertragen und zum Erstellen professioneller Berichte verwendet werden. AirCheck Manager kann Informationen von verschiedenen Testsitzungen vergleichen, um Änderungen in einem WLAN zu erkennen.

Registrieren des Produkts

Die Registrierung des Produkts bei Fluke Networks gewährleistet Zugang zu wertvollen Informationen über Produktaktualisierungen, Verfahren zur Fehlerbehebung und weitere Dienstleistungen. Zur Registrierung auf der Fluke Networks-Website unter **www.flukenetworks.com/MyAccountDE** das Online-Formular ausfüllen.

Fluke Networks-Wissensdatenbank

Die Fluke Networks-Wissensdatenbank enthält Antworten auf häufig gestellte Fragen zu Fluke Networks-Produkten und schließt Informationen über Technologie und Verfahren für Netzwerk- und Kabeltests ein. Um die Wissensdatenbank aufzurufen, besuchen Sie die Website **www.flukenetworks.com/de**, und klicken Sie auf **Support** > **Wissensdatenbank**.

Kontaktaufnahme mit Fluke Networks

www.flukenetworks.com/de

support@flukenetworks.com

+1-425-446-4519

- Australien: 61 (2) 8850-3333 oder 61 (3) 9329-0244
- Peking: 86 (10) 6512-3435
- Brasilien: 11 3759 7600
- Kanada: 1-800-363-5853
- Europa: +31-(0) 40 2675 600
- Hongkong: 852 2721-3228
- Japan: 03-6714-3117
- Korea: 82 2 539-6311
- Singapur: +65-6799-5566
- Taiwan: (886) 2-227-83199
- USA: 1-800-283-5853

Weitere Telefonnummern finden Sie auf unserer Website.

Sicherheitsinformationen

Tabelle 1 beschreibt die an diesem Tester und in diesem Handbuch verwendeten Sicherheitssymbole.

Tabelle 1. Sicherheitssymbole

	Warnung oder Vorsicht: Gefahr der Beschädigung oder Zerstörung von Geräten oder Software. Siehe Erklärungen im Handbuch.
	Warnung: Stromschlaggefahr.
	Produkte, die über Leiterplatten verfügen, dürfen nicht in Abfallbehältern entsorgt werden. Die Entsorgungsregelungen für Ihre Region entnehmen Sie bitte den örtlichen Bestimmungen und Vorschriften.
	Dieses Gerät enthält ein Klasse-2-Funkgerät.

⚠Warnung⚠

Den mitgelieferten Netzadapter nur zum Aufladen der Batterie verwenden.

⚠Vorsicht

Falls eine externe Antenne eingesetzt wird, ausschließlich die Antenne verwenden, die Fluke Networks für den AirCheck Tester herstellt. Der Tester funktioniert nicht korrekt mit anderen Antennen.

Auspacken

Der AirCheck Wi-Fi Tester wird mit dem unten aufgeführten Zubehör geliefert. Falls Teile fehlen oder beschädigt sind, sofort den Fachhändler verständigen, bei dem das Produkt gekauft wurde.

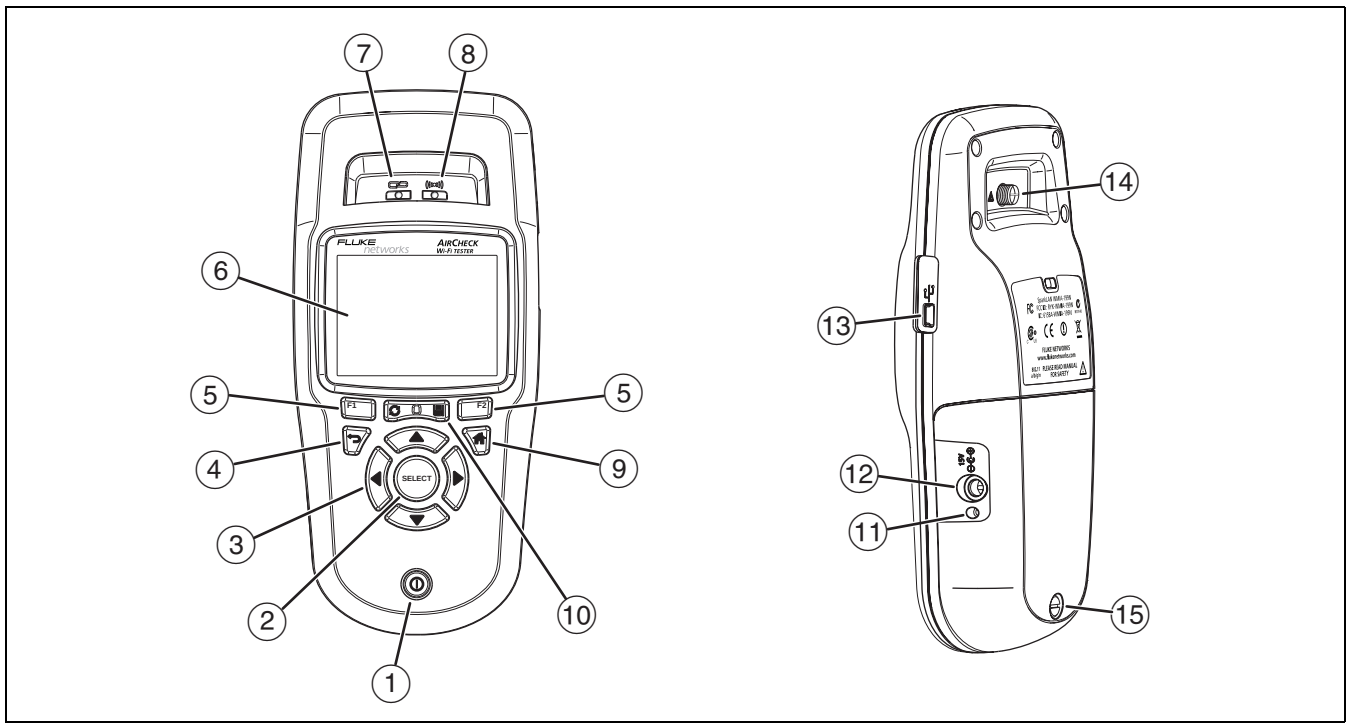
AirCheck Wi-Fi Tester

- AirCheck mit aufladbarem Batteriepack
- Netzadapter
- USB-Kabel
- Transportbehälter
- Erste Schritte-Anleitung
- Produkthandbücher-CD
- AirCheck Manager-Software-CD

AirCheck Frontline-Fehlerbehebungs-Kit

- AirCheck mit aufladbarem Batteriepack
- Extrabatteriepack
- LinkRunner™ Pro
- Externe Richtantenne mit RSMA-Steckverbinder
- PoE-Detektor
- Netzadapter
- USB-Kabel
- Transportbehälter
- Erste Schritte-Anleitung
- Produkthandbücher-CD
- AirCheck Manager-Software-CD

Äußere Merkmale



ffy01.eps

Abbildung 1. Äußere Merkmale

① Ein/Aus-Taste.

② Trifft eine Auswahl auf dem Bildschirm.

③ Navigationstasten.

④ Zeigt den vorherigen Bildschirm an.

⑤ Softkeys. Die Funktion des Softkeys wird oberhalb der Taste angezeigt.

⑥ LCD-Farbanzeige.

⑦ Die LED blinkt, wenn der Tester versucht, eine Verbindung zu einem WLAN herzustellen. Die LED ist an, wenn der Tester mit einem WLAN verbunden ist.

⑧ Die LED blinkt, wenn der Tester Daten überträgt.

⑨ Zeigt den Home-/Start-Bildschirm an.

⑩ : Löscht alle in der aktuellen Testsequenz erfassten Daten. Die im Speicher gespeicherten Ergebnisse werden dadurch nicht gelöscht. : Speichert alle Daten in einer Sitzungsdatei. Siehe Seite 62.

⑪ Die LED leuchtet auf, wenn der Netzadapter angeschlossen wird. Die LED leuchtet rot, wenn die Batterie aufgeladen wird, und grün, wenn die Batterie vollständig aufgeladen ist.

⑫ Anschluss für den Netzadapter.

⑬ USB-Anschluss für Verbindung zu einem PC.

⑭ Anschluss für die externe Richtantenne. Siehe Seite 58.

⑮ Schraube für das Batteriepack.

Laden und Betriebsdauer des Akkus

Vor dem erstmaligen Gebrauch den Akku 4 Stunden lang aufladen.

Um die Batterie aufzuladen, den Netzadapter an den Batterieanschluss anschließen (⑫ in Abbildung 1). Der Tester kann während des Aufladens der Batterie verwendet werden.

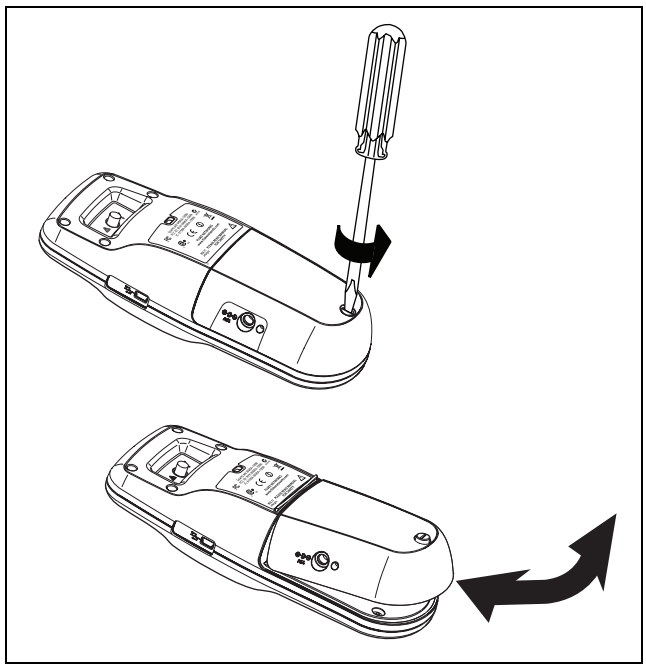
Abbildung 2 zeigt, wie die Batterie ersetzt wird.

Wenn der Tester ausgeschaltet ist, dauert das Aufladen der Batterie ungefähr 3 Stunden.

Hinweis

Die Batterie wird nicht aufgeladen, wenn die Innentemperatur des Testers 45 °C übersteigt.

Die Akku-Betriebsdauer beträgt bei normalem Betrieb etwa 5,5 Stunden. Ein Symbol oben links auf dem Bildschirm zeigt den Batteriezustand an. Siehe Abbildung 3 auf Seite 13.



ffy14.eps

Abbildung 2. Entfernen der Batterie

Mindestkonfiguration für bestmögliche Leistung

Um mit dem Tester optimale Leistung zu erzielen, mit AirCheck Manager ein Profil konfigurieren und auf den Tester übertragen. Ein Profil enthält Daten, die der Tester für folgende Aufgaben benötigt:

- Verbindung zu Netzwerken herstellen, die Sicherheitsdaten erfordern.
- Anzeigen des korrekten Autorisierungsstatus für jeden Access Point. So können Sie rasch erkennen, welche Access Points autorisierte Teile des Netzwerks sind.
- Pingen von wichtigen Netzwerkgeräten.

Siehe „Tester einrichten“ auf Seite 14.

Informationen über Netzwerke

Die folgenden Abschnitte bieten eine Übersicht über die Informationen, die der Tester in einer Netzwerkumgebung ausfindig machen kann.

Was befindet sich im WLAN?

Welche WLANs sind verfügbar?	Wählen Sie **Netzwerke** zum Anzeigen einer Liste der WLANs und Access Points, die mit jedem Netzwerk verbunden sind. Zum Anzeigen aller Access Points, die an Ihrem Standort verfügbar sind, wählen Sie **Access Points**. Siehe Seite 24.
Welche Access Points sind verfügbar? Sind die Signalstärken ausreichend?	Wählen Sie **Access Points** zum Anzeigen einer Liste der Access Points, die an Ihrem Standort verfügbar sind, und der Signalstärken der Access Points. Siehe Seite 28.
Ist der Access Point richtig konfiguriert?	Wählen Sie **Access Points**, markieren Sie einen Access Point, und drücken Sie dann SELECT. Siehe Seite 28.
Gibt es neue Access Points in der Umgebung? Gibt es Access Points, die nicht wahrnehmbar sind?	Speichern Sie die Testsitzung, und verwenden Sie den AirCheck Manager, um die Liste der Access Points mit einer anderen, im AirCheck Manager gespeicherten Liste zu vergleichen. Siehe Seiten 54 und 65.
Von welchen WLAN-Clients wird das Netzwerk genutzt?	Wählen Sie die Option **Tools** und anschließend die Option **Clients auflisten** aus. Siehe Seite 49.

Können Geräte eine Verbindung zum Netzwerk herstellen?

Benutzen Sie den Tester zum Prüfen der Netzwerkverbindung.

Hinweis

Um eine Verbindung mit einem sicheren Netzwerk herzustellen, benötigt der Tester ein Profil, welches Sicherheitsdaten beinhaltet. Falls keine Anmeldeinformationen verfügbar sind, wird der Softkey als F1 ***Verbinden**** *angezeigt. Siehe Seite 14.*

Kann ein Gerät als Client eine Verbindung zum Netzwerk (SSID) herstellen?	Wählen Sie **Netzwerke**, markieren Sie ein Netzwerk, und drücken Sie dann F1 **Verbinden**. Siehe Seite 42.
Kann ein Gerät eine Verbindung zu einem Access Point (BSSID) herstellen?	Wählen Sie **Access Points**, markieren Sie einen Access Point, und drücken Sie dann F1 **Verbinden**. Siehe Seite 42.
Wenn ein Gerät keine Verbindung zu einem Netzwerk oder Access Point herstellen kann, woran scheitert der Verbindungsvorgang?	Sehen Sie sich das Verbindungsprotokoll an. Siehe Seite 45.
Kann ein Gerät ein Netzwerkgerät pingen?	Führen Sie einen Ping-Test durch. Siehe Seite 46.
Funktioniert die Netzwerkkarte in einem Client korrekt?	Wählen Sie die Optionen **Tools** und dann **Clients auflisten** aus, um zu sehen, ob der Client Probe-Anforderungsframes überträgt, und um elementare Einstellungen wie den Kanal und die SSIDs anzuzeigen, die der Client in Proben verwendet. Siehe Seite 50.

Was ist der Grund für schwache Netzwerkleistung oder Verbindungsverluste?

Ist die Signalstärke ausreichend?	Wählen Sie **Access Points**. Der Bildschirm **Access Points** zeigt die Signalstärke für jeden einzelnen Access Point an. Wählen Sie einen Access Point, um mehr Details über Signalstärke und Auslastung anzuzeigen. Siehe Seite 32.
Ist das Netzwerk überlastet?	Wählen Sie **Kanäle**, um einen Überblick über die Kanalverwendung und die Anzahl der Access Points, die den jeweiligen Kanal verwenden, anzuzeigen. Um ein Diagramm anzuzeigen, markieren Sie einen Kanal, und drücken Sie SELECT. Siehe Seite 39.
Wird ein Kanal oder Access Point von zu vielen Clients verwendet?	Wählen Sie die Optionen **Tools** und anschließend **Clients auflisten** aus, um anzuzeigen, von wie vielen Clients ein Kanal oder Access Point verwendet wird. Siehe Seite 49.
Verwenden zu viele Clients niedrige Datenraten?	Wählen Sie die Optionen **Tools** und anschließend **Clients auflisten** aus, um die Datenraten für die Clients anzuzeigen. Siehe Seite 49.
Wird auf einem der Kanäle eine nicht-802.11-Störung angezeigt?	Wählen Sie **Kanäle**. Nicht-802.11-Störungen werden grau dargestellt. Das Störsignal kann sich auf die WLAN-Verbindung oder -Leistung auswirken. Nicht-802.11-Störungen können von Mikrowellenherden, drahtlosen Telefonen, Bluetooth®-Geräten, Bewegungsmeldern, drahtlosen Kameras und anderen drahtlosen Geräten ausgehen. Siehe Seite 40.

Weist das Netzwerk Sicherheitsrisiken auf?

Verfügen die Netzwerke über die erwartete Sicherheitsstufe?	Wählen Sie **Netzwerke**. Netzwerke mit ungesicherten Access Points sind durch ein offenes rotes Schloss ( ) gekennzeichnet. Siehe Seite 24.
Gibt es in der Umgebung Ad hoc-Netzwerke?	Wählen Sie **Netzwerke**. Netzwerke mit Ad Hoc-Clients sind durch das Ad Hoc-Symbol ( ) in der **SSID**-Spalte gekennzeichnet. Ad Hoc-Clients können ein Risiko für die Sicherheit des Netzwerks darstellen bzw. gegen Netzwerkrichtlinien verstoßen. Siehe Seite 24.
Gibt es nicht autorisierte Access Points in der Umgebung? Wo befinden sich diese?	Der Status von Access Points wird als „ **Nicht autorisiertes Gerät**“ angezeigt, bis Sie ihn verändern. Wenn Sie allen Access Points im Netzwerk einen Status zuordnen, werden die neuen, möglicherweise nicht autorisierten Access Points durch den Status gekennzeichnet. Wenn bekannt ist, dass es sich bei einem Access Point um einen unautorisierten Zugangspunkt handelt, kann der Status „ **Markiertes Gerät**“ zugeordnet werden. Siehe Seite 22. Zum Anzeigen des Autorisierungsstatus wählen Sie **Access Points**, markieren Sie einen Access Point, und drücken Sie dann F2 **ACL**. Zum Auffinden eines Access Points, den Zugangspunkt auswählen und dann F2 **Orten** auf dem Bildschirm **Access Point-Details** drücken. Siehe Seite 54.

Wo befindet sich ein Access Point?

Wählen Sie **Access Points**, wählen Sie einen Access Point, und drücken Sie dann F2 **Orten** im Bildschirm **Access Point-Details**. Siehe Seite 54. Benutzen Sie die optionale externe Richtantenne von Fluke Networks, um Access Points schneller ausfindig zu machen. Siehe Seite 58.

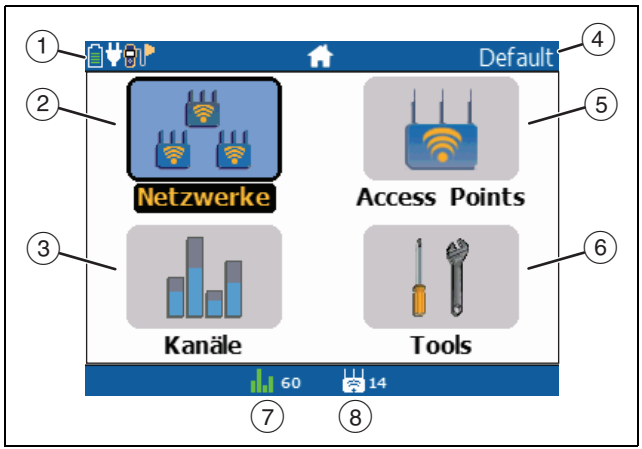
Welche Netzwerke oder Access Points kommen bei Bewegung in Reichweite?

Für die Zeitstempelspalte (🕒) die Liste in absteigender Folge sortieren. 🔄 drücken und dann einen Bereich abschreiten. Netzwerke oder Access Points, die in Reichweite kommen, werden der Liste oben hinzugefügt. Siehe Seite 25 oder 29.

Wie kann ich mein Netzwerk und meine Testsitzung dokumentieren?

Die Sitzung speichern (siehe Seite 54) und dann die AirCheck Manager-Software verwenden, um die Daten auf einen PC zu übertragen und einen Bericht zu erstellen. Siehe Seite 65.

HOME-Bildschirm (Startbildschirm)



gdk15.eps

Abbildung 3. HOME-Bildschirm (Startbildschirm)

(1) Zeigt den Ladezustand des Akkus an. Bei schwacher Akkuladung blinkt das Symbol. Den Netzadapter anschließen, um die Batterie aufzuladen und fortdauernden Betrieb des Testers zu gewährleisten.

Zeigt an, dass das Netzteil angeschlossen ist.

Zeigt an, dass die externe Antenne angeschlossen ist.

(2) **Netzwerke**: Ermittelt WLANs. Siehe Seite 23.

(3) **Kanäle**: Zeigt die Auslastung von WLAN-Kanälen an. Siehe Seite 38.

(4) Der Name des vom Tester verwendeten Profils. Das Profil ist **Default**, falls kein anderes Profil geladen wurde. Der Name erscheint mit einem Sternchen, wenn seit dem Laden/Speichern des Profils eine Einstellung auf dem Tester verändert wurde. Siehe Seite 64.

(5) **Access Points**: Ermittelt Access Points. Siehe Seite 23.

(6) **Tools**: Ermöglicht die Verwaltung von Dateien und Einstellungen. Enthält auch eine Liste von Clients, die Proben übertragen (siehe Seite 49).

(7) Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

(8) Die Anzahl der Access Points, die der Tester ermittelt hat. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 17.

Tester einrichten

Um die Einstellungen auf dem Tester zu ändern, **Tools** auf dem Startbildschirm auswählen. Siehe Tabelle 2 auf Seite 17.

Ändern der Sprach- und Landeseinstellungen

1 **Tools** auswählen.

2 Um die Sprache für die Bildschirme zu ändern, **Set Language (Sprache einstellen)** auswählen. Eine Sprache markieren und dann F2 **Save (Speichern)** drücken.

3 Um das Land zu ändern, **Land einstellen** auswählen und dann das Land auswählen, in dem der Tester verwendet wird. Siehe Seite 19.

Erstellen eines Profils für Verbindungen zu gesicherten Netzwerken

Profile sind Dateien, die die Einstellungen für Netzwerke und den Tester enthalten. Zu den Netzwerkeinstellungen gehören Sicherheitsanmeldeinformationen. Sicherheitsanmeldeinformationen ermöglichen dem Tester, Verbindungen zu Netzwerken herzustellen und Ping-Tests durchzuführen. Profile können Kennwörter aufweisen, sodass nicht autorisierte Benutzer in AirCheck Manager keinen Zugriff auf Netzwerksicherheitsanmeldeinformationen haben und den Tester nicht für Verbindungen zu gesicherten Netzwerken verwenden können.

Die Einstellungen des Testers können als Profil gespeichert werden. Profile können auch mit AirCheck Manager auf einem PC erstellt werden.

Der Startbildschirm zeigt den Namen des vom Tester verwendeten Profils an. Der Name erscheint mit einem Sternchen, wenn seit dem Laden/Speichern des Profils eine Einstellung auf dem Tester verändert wurde. Der Tester speichert die Änderungen in einer temporären Datei; dabei handelt es sich um eine Kopie des auf dem Startbildschirm angezeigten Profils. Der Tester verwendet die temporäre Datei als das aktuelle Profil. Wenn das Profil gespeichert wird, kopiert der Tester die Änderungen in das auf dem Startbildschirm angezeigte Profil.

In AirCheck Manager erstellte Profile enthalten diese Einstellungen:

- Ein Kennwort für das Profil
- Sicherheitsanmeldeinformationen für Netzwerke

  Hinweis

  Um ein Profil zu erstellen, das Sicherheitsanmeldeinformationen für ein Netzwerk oder ein Kennwort für das Profil einschließt, muss AirCheck Manager verwendet werden.

- IP-Adressen und der Autorisierungsstatus von Netzwerken (SSIDs) und Access Points

- IP-Adressen für Ping-Tests
- Alle 802.11-Einstellungen (z.B. **2,4 GHz-Band aktivieren** und **5 GHz-Band aktivieren**. Siehe Seite 17.)
- Land
- Audioeinstellung für Ortungsfunktion

Wenn das Profil gespeichert wird, während es auf dem Tester aktiviert ist, fügt der Tester diese Einstellungen zum Profil hinzu:

- Audioeinstellung für Ortungsfunktion
- Einstellung für automatische Abschaltung
- Sequenzen für die Sortierreihenfolge für Listen von Netzwerken, Access Points und Clients

Übertragen eines Profils von einem PC auf den Tester

1 Den **Profil-Manager** in AirCheck Manager verwenden, um ein Profil zu erstellen.

2 Das gelieferte USB-Kabel verwenden, um den Tester am PC anzuschließen.

3 Die Funktion **übertragen** im **Profil-Manager** verwenden, um das Profil auf den Tester zu übertragen.

Laden eines Profils, das sich auf dem Tester befindet

1 **Tools** > **Dateien verwalten** und dann **Profil laden** auswählen.

2 Ein Profil hervorheben, SELECT drücken und dann F2 **Laden** drücken.

Hinweis

Falls die Datei kein gültiges Profil ist, oder die Erweiterung nicht „.ACP" lautet, zeigt der Tester die Meldung „Ausg.Profil n.ladbar." an.

3 Ggf. das Kennwort für das Profil eingeben.

Hinweis

Das Kennwort muss nur beim ersten Mal eingegeben werden, wenn ein Profil auf den Tester geladen wird. Um Kennwortschutz auf allen Profilen zu reaktivieren ***Tools*** *>* ***Werkseit.Standardeinst.wiederherst.*** *auswählen.*

Speichern der aktuellen Einstellungen als Profil

1 **Tools** > **Dateien verwalten** auswählen und dann **Profil speichern** auswählen.

- Um die Profile mit dem angegebenen Dateinamen zu speichern, F2 **Speichern** drücken. Der Tester speichert das Profil im „PROFILES"-Ordner.
- Um ein auf dem Tester gespeichertes Profil zu überschreiben, das Profil hervorheben, SELECT drücken, F2 **Speichern** drücken und dann F2 **OK** drücken.
- Um den Dateinamen zu bearbeiten, F1 **Bearbeiten** drücken.

Hinweis

Dateinamen können maximal 8 Zeichen und eine Erweiterung von 3 Zeichen umfassen. Die Erweiterung muss „.ACP" lauten, wenn das Profil in AirCheck Manager erscheinen soll.

- Um Zeichen innerhalb des Dateinamens zu löschen, F1 **Löschen** drücken.
- Um Zeichen zum Dateinamen hinzuzufügen, ▲▼◀▶ verwenden, um ein Zeichen hervorzuheben, und dann SELECT drücken.
- Um den Cursor im Dateinamen zu verschieben, den Dateinamen hervorheben und dann ◀▶ drücken.
- Um das Profil unter dem bearbeiteten Dateinamen zu speichern, F2 **Fertig** drücken und dann F2 **Speichern** drücken. Der Tester speichert das Profil im „PROFILES"-Ordner.

Einstellungen

Tabelle 2 enthält die Einstellungen, die im Menü **Tools** vorgenommen werden können.

Wenn eine Einstellung verändert wurde, F2 **Speichern** drücken, um die Einstellungen zu speichern. Um ohne Speicherung der Einstellungen zu beenden, F1 **Abbrechen** drücken.

Hinweis

Um die Einstellungen in einem Profil zu speichern, ***Tools*** *>* ***Profil speichern*** *auswählen.*

Tabelle 2. Einstellungen im Menü „Tools“

802.11-Einstellungen verwalten *Hinweis* *Diese Einstellungen ändern die Art und Weise, wie der Tester Access Points ermittelt und anzeigt. Vor Gebrauch des Testers sicherstellen, dass bekannt ist, was diese Einstellungen bewirken.*	Ermöglicht das Festlegen von Optionen für Kanäle und Access Point-Listen. • **2,4 GHz-Band aktivieren, 5 GHz-Band aktivieren**: Ein oder beide Frequenzbänder auswählen, um entsprechende Netzwerke und Access Points anzuzeigen. • **Proben übertragen**: Um Access Points zu ermitteln, achtet der Tester auf jedem Kanal auf SSID-Broadcasts. Der Tester kann nur Access Points ermitteln, die ihre SSID aussenden, während der Tester auf dem gleichen Kanal eingeschaltet ist. Für schnellere Ermittlung überträgt der Tester standardmäßig Probe-Request-Frames, um Antworten von Access Points zu erhalten. Da Proben die Kanalauslastung erhöhen, überträgt der Tester keine Proben, wenn der Kanalauslastungsbildschirm angezeigt wird, oder wenn die externe Antenne angeschlossen wird.

-Fortsetzung-

Tabelle 2. Einstellungen im Menü „Tools“ (Fortsetzung)

802.11-Einstellungen verwalten (Fortsetzung) *Hinweis* *Diese Einstellungen ändern die Art und Weise, wie der Tester Access Points ermittelt und anzeigt. Vor Gebrauch des Testers sicherstellen, dass bekannt ist, was diese Einstellungen bewirken.*	• **Virtuelle Access Points gruppieren**: Wenn ein Access Point mehrere MAC-Adressen (**BSSIDs**) aussendet, stellen die MAC-Adressen virtuelle Access Points dar. Virtuelle Access Points können verschiedene Netzwerke vom gleichen physischen Access Point aus unterstützen. Ein Access Point, der zwei Funkgeräte verwendet, um mehrere MAC-Adressen auszusenden, kann Netzwerke auf unterschiedlichen Kanälen unterstützen. Wenn **Virtuelle Access Points gruppieren** aktiviert ist, werden virtuelle Zugangspunkte in der **Access Points**-Liste als ein Access Point angezeigt. Wenn der Access Point einen Namen aussendet (angezeigt in der Spalte **Name/MAC**), wird die Anzahl der unterstützten SSIDs in der Spalte **SSID** angezeigt. Zum Beispiel wird „**2 SSIDs**“ in der Spalte angezeigt. Wenn der Access Point keinen Namen aussendet, hat er ein Sternchen als letzte Stelle der MAC-Adresse in der **Name/MAC**-Spalte. Um die MAC-Adressen und die **SSIDs** für die virtuellen Access Points anzuzeigen, den Access Point in der **Access Points**-Liste auswählen. Diese Einstellung ist standardmäßig aktiviert. • **Nicht hörbare APs ausgrauen:** Wenn der Tester einen Access Point während vier Zyklen über alle Kanäle nicht wahrnimmt, wird der Access Point in der **Access-Points**-Liste grau dargestellt. Dies ist die Standardeinstellung. • **Nicht hörbare Access Points löschen**: Wenn der Tester einen Access Point während vier Zyklen über alle Kanäle nicht wahrnimmt, wird der Access Point in der **Access-Points**-Liste gelöscht.

Tabelle 2. Einstellungen im Menü „Tools“ (Fortsetzung)

Benutzerdef. Signalanpassung verwenden	Ermöglicht, Signalstärkemessungen so einzustellen, dass sie mit anderen Geräten übereinstimmen. Siehe Seite 61.
Datum und Uhrzeit einstellen	Ermöglicht das Einstellen des Datums und der Uhrzeit. Der Tester fügt Zeitstempel zu gespeicherten Ergebnissen hinzu. ◀▶ verwenden, um eine Einstellung auszuwählen, und dann ▼▲ verwenden, um die Einstellung zu ändern.
Schwellenwerte einstellen	Ermöglicht die Einstellung der Schwellenwerte für die Farben in Balkendiagrammen von Messungen. Siehe Seite 21.
Land einstellen	Kanäle, die im ausgewählten Land illegal sind, werden auf den Bildschirmen **Kanalverwendung**, **Details zur Kanalverw.** und **Access Point-Details** rot dargestellt. Siehe „802.11d-Betrieb“ auf Seite 20. Access Points, die einen Ländercode übertragen, der nicht mit dieser Einstellung übereinstimmt, weisen in der Spalte **802.11** rote Balken auf.
Sprache einstellen	Ändert die Sprache der Benutzeroberfläche.
Strommanagement	Wenn diese Option aktiviert ist, schaltet der Tester sich automatisch aus, wenn 10 Minuten lang keine Taste gedrückt wird. Der Tester speichert die Testsitzung nicht, wenn er automatisch ausschaltet. Im Profil vorgenommene Änderungen werden ebenfalls nicht gespeichert. Der Tester schaltet sich nicht automatisch aus, wenn der Netzadapter angeschlossen ist. Um die Einstellung zu speichern, F2 **Speichern** drücken. Um ohne Speicherung der Einstellungen zu beenden, F1 **Abbrechen** drücken.
Werkseit. Standardeinst. wiederherst.	Setzt alle Einstellungen auf Standardwerte zurück. Siehe Anhang B.

802.11d-Betrieb

Wenn ein Access Point den 802.11d-Standard verwendet, überträgt er einen ISO-Ländercode in seinen Beacons- und Probe-Antworten. Wenn der Tester diesen Code empfängt, überträgt er nur auf Kanälen, die in dem Land legal sind, und er verwendet nur Leistungspegel, die legal sind.

Wenn der Tester keinen Ländercode empfängt, funktioniert er im „Weltmodus“.

- Der Tester verwendet nur Kanäle und Leistungspegel, die in allen Ländern legal sind. Die Kanäle lauten 1 bis 11 im 2,4 GHz-Band.
- Der Tester überträgt keine Proben auf den Kanälen 12, 13 und 14 im 2,4 GHz-Band.
- Der Tester überträgt keine Proben im 5 GHz-Band, es sei denn, er erkennt Access Points, die in diesem Band funktionieren.
- Der Tester verwendet die niedrigste Übertragungsleistung, die in allen Ländern legal ist.

Die Balken am unteren Rand der Anzeige und die Symbole auf den Netzwerk- und Access Point-Anzeigen zeigen den Status des Ländercodes an:

Grüne Balken: Der Tester hat einen Ländercode von einem oder mehreren Access Points empfangen. Alle empfangenen Ländercodes sind gleich und stimmen mit der Einstellung unter **Tools** > **Land einstellen** überein. Der Tester verwendet nur Kanäle und Leistungspegel, die in diesem Land legal sind.

Weiße Balken: Der Tester hat keinen Ländercode empfangen. Der Tester funktioniert im Weltmodus.

Rote Balken: Der Tester hat einen Ländercode empfangen, der sich von der Einstellung unter **Tools** > **Land einstellen** unterscheidet. Um das Netzwerk bzw. den Access Point zu ermitteln, das/der diesen Code überträgt, **Netzwerke** bzw. **Access Points** auswählen und dann auf die roten Balken in der **802.11**-Spalte achten.

Der Bildschirm **Access Point-Details** zeigt den 802.11d-Ländercode an, der vom Access Point übertragen wird. Anhang C enthält die Länder und die Codes.

Ändern der Schwellenwerte für die Farben in Balkendiagrammen

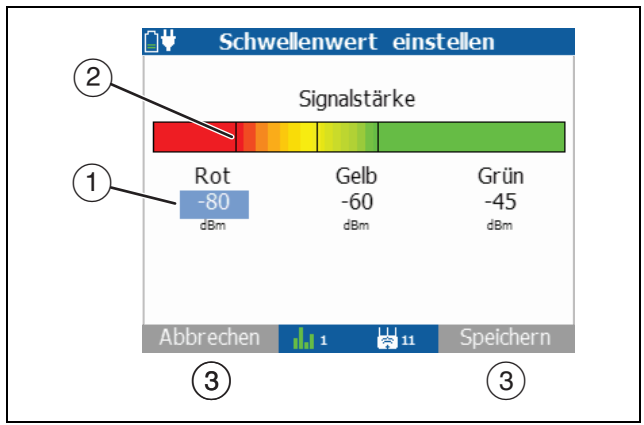
Die Farben der Balkendiagramme zeigen an, ob die Signalstärke, die Störstärke und das Signal-Rausch-Verhältnis (SNR) oberhalb oder unterhalb der spezifizierten Schwellenwerte liegen. Die Schwellenwerte können verändert werden, sodass die Farben angezeigt werden, wenn das Signal die Anforderungen des jeweiligen Netzwerks erfüllt.

Ändern der Schwellenwerte für die Farben

1 **Tools** auswählen.

2 **Schwellenwerte einstellen** auswählen.

3 Ein Element auswählen. Abbildung 4 zeigt, wie die Schwellenwerte für die Farben verändert werden.



gdk05.eps

Abbildung 4. Ändern der Schwellenwerte für die Farben in einem Balkendiagramm

(1) ◀▶ verwenden, um eine Farbe auszuwählen. ▲▼ verwenden, um den Messwert für diese Farbe zu erhöhen bzw. zu reduzieren.

(2) Die Linien zeigen an, wo die eingestellten Werte auf dem Balkendiagramm liegen.

(3) Um die Einstellungen zu speichern, F2 **Speichern** drücken. Um ohne Speicherung der Einstellungen zu beenden, F1 **Abbrechen** drücken.

Zuordnen eines Autorisierungsstatus zu Access Points

Wenn den einzelnen Access Points ein Autorisierungsstatus zugeordnet wird, kann man schnell erkennen, ob ein Access Point autorisierter Teil des Netzwerks ist. Access Points haben ein gelbes Dreieck (⚠) in der Zugriffskontrollliste-Spalte (**ACL**), bis der Status verändert wird.

Zuordnen eines Autorisierungsstatus zu einem Access Point

1 Wählen Sie **Access Points**.

2 Wenn ein Access Point mehr als eine MAC-Adresse aufweist und den einzelnen MAC-Adressen unterschiedliche Autorisierungsstati zugeordnet werden sollen, den Access Point auswählen.

3 Einen Access Point hervorheben und dann F2 **ACL** (Access Control List = Zugriffskontrollliste) drücken.

4 Auf dem Bildschirm **Autorisierungsstatus** einen Status hervorheben, SELECT drücken und dann ↵ drücken.

⚠ **Nicht autorisiertes Gerät**: Dem Access Point ist kein Autorisierungsstatus zugeordnet.

✓ **Autorisiertes Gerät**: Der Access Point ist für den Anschluss an das Netzwerk autorisiert

Nachbargerät: Der Access Point ist nicht für den Anschluss an das Netzwerk autorisiert, stellt jedoch für die Netzwerksicherheit keine Gefahr dar.

Gastgerät: Der Access Point ist für den Anschluss an das Netzwerk autorisiert, verfügt jedoch über begrenzten Zugriff.

Markiertes Gerät: Dieses Symbol kann für Access Points verwendet werden, die überwacht werden sollen. Wenn beispielsweise vermutet wird, dass ein Access Point unautorisiert ist, kann er mit einer Markierung versehen werden, bis mehr über den Access Point bekannt ist.

Wenn der Tester ausgeschaltet wird, werden die ACL-Einstellungen im temporären Profil gespeichert.

Hinweis

Wenn ein Access Point nicht überträgt und dessen MAC-Adresse bekannt ist, AirCheck Manager verwenden, um dem Access Point einen Autorisierungsstatus zuzuordnen. Den Status in einem Profil speichern und dann das Profil auf den Tester transferieren.

Erkennen von Netzwerken und Access Points

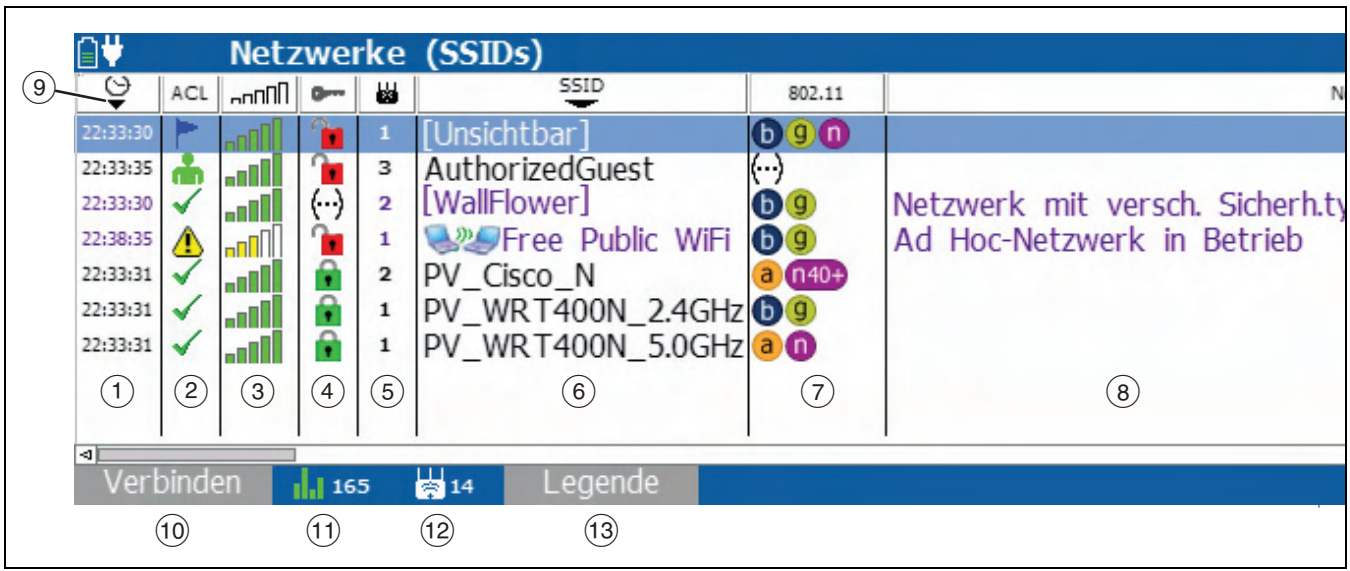
Hinweis

Der Tester sucht standardmäßig nach Wireless-Signalen auf den 2,4 GHz (b/g/n)- und 5 GHz (a/n)-Frequenzbändern, um Wireless Access Points zu ermitteln. Um diese Einstellung zu ändern, ***Tools*** *auswählen und dann* ***802.11-Einstellungen verwalten*** *auswählen.*

Ermitteln von Netzwerken bzw. Access Points

1 Auf dem Startbildschirm **Netzwerke** oder **Access Points** auswählen. Der Tester zeigt die Liste **Netzwerke** oder die Liste **Access Points** an (Abbildungen 5 und 6).

2 Um Details über einen Access Point (Abbildung 7) anzuzeigen, ◁▷ verwenden, um den Access Point hervorzuheben, und dann SELECT drücken.



gdk03.eps

Abbildung 5. Netzwerke (SSIDs)

① : Der Zeitpunkt der ersten Wahrnehmung des Netzwerks durch den Tester. Zum Anzeigen von Netzwerken, die in Reichweite kommen wenn Sie sich durch ein Gebiet bewegen, sortieren Sie die Liste absteigend entsprechend der Spalte „Zeitstempel“.

Drücken Sie , und bewegen Sie sich durch ein Gebiet. Netzwerke, die in Reichweite kommen, werden der Liste oben hinzugefügt. Netzwerke, die außer Reichweite kommen, werden grau, wenn die Option **Nicht hörbare APs ausgrauen** aktiviert ist.

② **ACL**: Autorisierungsstatus des Access Point. Der Standardstatus ist **Nicht autorisiertes Gerät**. Ändern Sie den Status jedes Access Points, um anzuzeigen, wie er mit dem Netzwerk verbunden ist. Siehe Seite 22.

(...): Nicht alle Access Points im Netzwerk haben denselben Autorisierungsstatus.

③ : Die maximale Signalstärke aller Access Points für eine Netzwerk-**SSID**. Die Schwellenwerte für die Farben in den Balkendiagrammen können verändert werden. Siehe Seite 21.

④ : Der Sicherheitsstatus des Netzwerks:

Rotes geöffnetes Schloss: Die Sicherheit ist für das Netzwerk nicht aktiviert.

Gelbes geschlossenes Schloss: Ein oder mehrere Access Points verwenden WEP- oder Cisco LEAP-Sicherheitsprotokolle. Diese sind weniger sicher als andere Protokolle.

Grünes geschlossenes Schloss: Alle Access Points verwenden Sicherheitsprotokolle, die sicherer sind als WEP, z. B. WPA oder WPA2.

(...): Nicht alle Access Points im Netzwerk verwenden dieselbe Sicherheitsverschlüsselung. Beispielsweise verwendet der eine WEP und der andere WPA.

⑤ : Die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points.

⑥ **SSID**: Service Set Identifier. Der Name des Drahtlosnetzwerks.

Netzwerke, die in letzter Zeit vom Tester nicht wahrgenommen wurden, werden grau dargestellt, falls **Nicht hörbare APs ausgrauen** aktiviert ist (siehe Seite 18).

: Das Netzwerk verfügt über Ad hoc-Geräte. Diese Geräte können direkt, ohne einen Access Point, der Teil des Netzwerks ist, mit anderen Geräten kommunizieren. Über Ad hoc-Geräte können sich Hacker Zugang zu Daten verschaffen, die im Netzwerk übertragen werden. (Einige IT-Richtlinien für Netzwerke lassen Ad hoc-Geräte zu.)

[Unsichtbar]: Die SSID des Netzwerks wird nicht gesendet.

Wenn eine SSID in eckigen Klammern angezeigt wird, hat der Tester die unsichtbare SSID in Paketen von anderen WLAN-Clients ermittelt. In AirCheck Manager werden diese SSIDs ohne eckige Klammern angezeigt.

⑦ **802.11**: Die von den Access Points im Netzwerk verwendeten 802.11-Standards:

802.11a: Verwendet das 5 GHz-Band.

802.11b: Verwendet das 2,4 GHz-Band.

802.11g: Verwendet das 2,4 GHz-Band.

802.11n: Kann mit 2,4 GHz- oder 5 GHz-Band verwendet werden.

Rote Balken: Der Tester hat einen 802.11d-Ländercode vom Access Point empfangen. Das Land stimmt nicht mit der Einstellung im Tester unter **Tools** > Land einstellen überein.

: Ein oder mehrere Access Points verwenden einen verbundenen Übertragungskanal. Access Points, die den 802.11n-Standard verwenden, können einen Übertragungskanal mit einem zusätzlichen Kanal darüber () oder darunter () verbinden, sodass ein 40 MHz-Übertragungskanal entsteht. Durch diesen breiteren Kanal wird ein höherer Durchsatz im Netzwerk möglich.

(...): Nicht alle Access Points im Netzwerk verwenden denselben 802.11-Standard.

⑧ **Notes (Notizen)**: Drücken Sie , um zum Feld „Notizen“ zu blättern. Der Tester fügt automatisch Notizen hinzu. Siehe Seite 35. Netzwerke mit Notizen erscheinen violett.

(...): Das Netzwerk verfügt über mehrere Notizen. Um alle Notizen anzuzeigen, das Netzwerk hervorheben und dann zweimal drücken, um zum Bildschirm **Access Point-Details** zu springen.

⑨ : **Sortieren 1**, absteigende und aufsteigende Reihenfolge

: **Sortieren 2**, absteigende und aufsteigende Reihenfolge

Um die Liste in aufsteigender oder absteigender Reihenfolge zu sortieren, und verwenden, um eine Spaltenüberschrift zu markieren, und dann bzw. **Sortieren 1** drücken. Um beispielsweise rasch den Access Point mit dem stärksten Signal zu finden, oben in der Spalte markieren und dann bzw. **Sortieren 1** drücken. Dadurch wird der Access Point mit dem stärksten Signal ganz oben in der Liste angezeigt.

Um in einer zweitrangigen Reihenfolge zu sortieren, markieren Sie einen anderen Spaltentitel und drücken Sie dann **Sortieren 2**.

⑩ Drücken Sie **Verbinden**, um eine Verbindung zum markierten Netzwerk herzustellen. Siehe Seite 42.

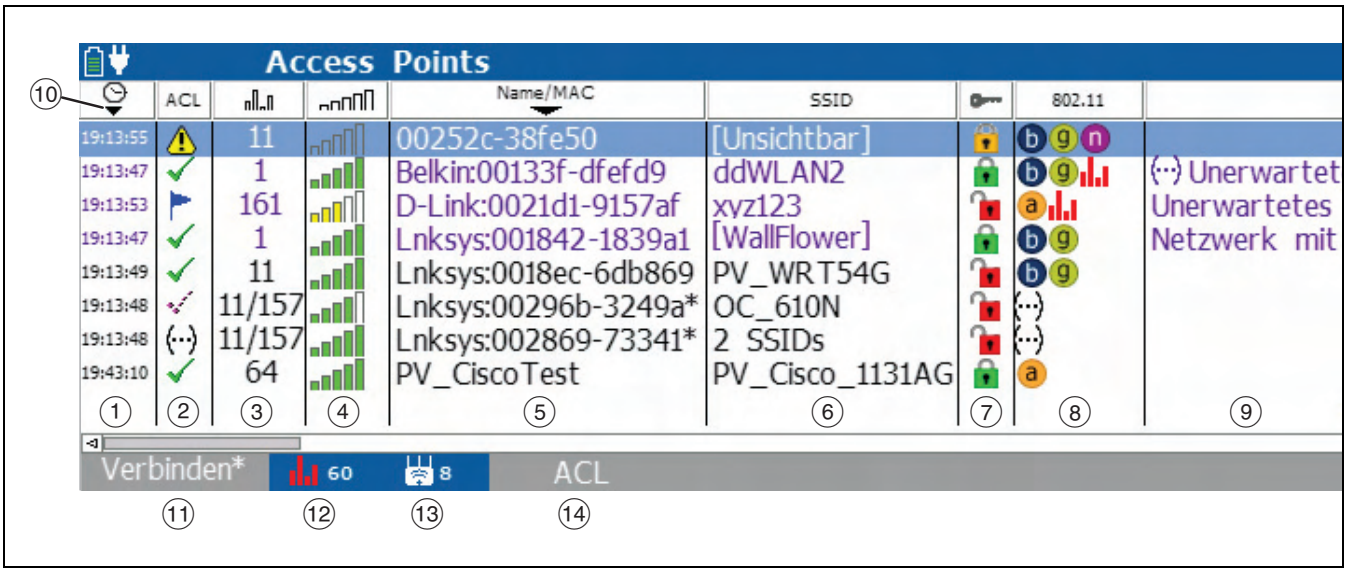
Die Schaltfläche „Verbinden“ wird als „**Verbinden***“ angezeigt, wenn der Tester keine Verbindung zum markierten Netzwerk herstellen kann. Siehe Seite 42.

⑪ : Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑫ : Die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 17.

⑬ Um die Beschreibungen der Symbole des Bildschirms **Netzwerke** anzuzeigen, drücken Sie **Legende**.

Um Details der Access Points im Netzwerk anzuzeigen, verwenden Sie zum Markieren des Netzwerks, und drücken Sie dann . Siehe Abbildung 6.



gdk02.esp

Abbildung 6. Access Points-Liste

① : Der Zeitpunkt der ersten Wahrnehmung des Access Point durch den Tester. Um Access Points anzuzeigen, die in Reichweite kommen, wenn ein Bereich abgeschritten wird, die Liste anhand der Zeitstempelspalte absteigend sortieren.

Drücken Sie , und bewegen Sie sich durch ein Gebiet. Access Points, die in Reichweite kommen, werden der Liste oben hinzugefügt. Access Points, die außer Reichweite gelangen, werden grau dargestellt, falls **Nicht hörbare APs ausgrauen** aktiviert ist.

② **ACL**: Autorisierungsstatus des Access Points. Der Standardstatus ist **Nicht autorisiertes Gerät**. Ändern Sie den Status jedes Access Points, um anzuzeigen, wie er mit dem Netzwerk verbunden ist. Siehe Seite 22.

(...): Virtuelle Access Points bzw. MAC-Adressen vom gleichen Access Point haben unterschiedliche Autorisierungsstatuseinstellungen. Normalerweise wird ihnen der gleiche Autorisierungsstatus zugeordnet.

③ : Der Kanal, der vom Access Point verwendet wird.

④ : Die Stärke des Signals. Bei mehreren APs zeigt diese Spalte die höchste Signalstärke an. Die Schwellenwerte für die Farben in den Balkendiagrammen können verändert werden. Siehe Seite 21.

⑤ **Name/MAC**: Der Name oder die MAC-Adresse des Access Points. Die Adresse beginnt mit einem Hersteller-Abkürzungspräfix, falls der Präfix verfügbar ist. Siehe „oui_abbr.txt“ auf Seite 64.

*****: Der Access Point sendet mehr als eine MAC-Adresse (BSSID) aus. Um die MAC-Adresse anzuzeigen, den Access Point auswählen. Siehe **„Virtuelle Access Points gruppieren“** auf Seite 18.

Access Points, die in letzter Zeit vom Tester nicht wahrgenommen wurden, werden grau dargestellt, falls **Nicht hörbare APs ausgrauen** aktiviert ist (siehe Seite 18).

⑥ **SSID**: Service Set Identifier. Die Kennung des Netzwerks.

Wenn der Access Point mehr als eine SSID unterstützt, den Access Point auswählen, um die SSIDs zu sehen. Siehe **„Virtuelle Access Points gruppieren“** auf Seite 18.

Wenn dieser Bildschirm vom Bildschirm **Netzwerke** aus abgerufen wird, wird die SSID zuoberst angezeigt.

Netzwerke, die in letzter Zeit vom Tester nicht wahrgenommen wurden, werden grau dargestellt, falls **Nicht hörbare APs ausgrauen** aktiviert ist (siehe Seite 18).

: Das Netzwerk verfügt über Ad hoc-Geräte. Diese Geräte können direkt, ohne einen Access Point, der Teil des Netzwerks ist, mit anderen Geräten kommunizieren. Über Ad hoc-Geräte können sich Hacker Zugang zu Daten verschaffen, die im Netzwerk übertragen werden. (Einige IT-Richtlinien für Netzwerke lassen Ad hoc-Geräte zu.)

[Unsichtbar]: Die SSID des Netzwerks wird nicht gesendet.

Wenn eine SSID in eckigen Klammern angezeigt wird, hat der Tester die unsichtbare SSID in Paketen von anderen WLAN-Clients ermittelt. In AirCheck Manager werden diese SSIDs ohne eckige Klammern angezeigt.

⑦ : Der Sicherheitsstatus des Access Point.

Rotes geöffnetes Schloss: Die Sicherheit ist für den Access Point nicht aktiviert.

Gelbes geschlossenes Schloss: Der Access Point verwendet das WEP-Sicherheitsprotokoll.

Grünes geschlossenes Schloss: Der Access Point verwendet ein Sicherheitsprotokoll, das sicherer ist als WEP, z. B. WPA oder WPA2.

: Der Access Point ist ein Ad Hoc-Gerät. Diese Geräte können direkt, ohne einen Access Point, der Teil des Netzwerks ist, mit anderen Geräten kommunizieren. Über Ad hoc-Geräte können sich Hacker Zugang zu Daten verschaffen, die im Netzwerk übertragen werden. (Einige Richtlinien für Netzwerke lassen Ad Hoc-Geräte zu.)

(...): Nicht alle Access Points verwenden dieselbe Sicherheitsverschlüsselung. Beispielsweise verwendet der eine WEP und der andere WPA.

⑧ **802.11**: Die 802.11-Standards, die vom Access Point verwendet werden:

: 802.11a: Verwendet das 5 GHz-Band.

: 802.11b: Verwendet das 2,4 GHz-Band.

: 802.11g: Verwendet das 2,4 GHz-Band.

: 802.11n: Kann mit 2,4 GHz- oder 5 GHz-Band verwendet werden.

Rote Balken: Der Tester hat einen 802.11d-Ländercode vom Access Point empfangen. Das Land stimmt nicht mit der Einstellung im Tester unter **Tools** > **Land einstellen** überein.

n 40+ n 40–: Access Points, die den 802.11n-Standard verwenden, können einen Übertragungskanal mit einem zusätzlichen Kanal darüber (n 40+) oder darunter (n 40–) verbinden, sodass ein 40 MHz-Übertragungskanal entsteht. Durch diesen breiteren Kanal wird ein höherer Durchsatz im Netzwerk möglich.

(...): Nicht alle Access Points verwenden denselben 802.11-Standard.

⑨ **Notes (Notizen)**: Drücken Sie ▸, um zum Feld „Notizen" zu blättern. Der Tester fügt automatisch Notizen hinzu. Siehe Seite 35. Access Points mit Notizen erscheinen violett.

(...): Der Access Point weist mehrere Notizen auf. Um alle Notizen einzusehen, den Bildschirm **Access Point-Details** abrufen.

⑩ : **Sortieren 1**, absteigende und aufsteigende Reihenfolge

: **Sortieren 2**, absteigende und aufsteigende Reihenfolge

Um die Liste in aufsteigender oder absteigender Reihenfolge zu sortieren, und verwenden, um eine Spaltenüberschrift zu markieren, und dann bzw. F1 **Sortieren 1** drücken. Um beispielsweise rasch den Access Point mit dem stärksten Signal zu finden, oben in der Spalte markieren und dann bzw. F1 **Sortieren 1** drücken. Dadurch wird der Access Point mit dem stärksten Signal ganz oben in der Liste angezeigt.

Um in einer zweitrangigen Reihenfolge zu sortieren, markieren Sie einen anderen Spaltentitel und drücken Sie dann F2 **Sortieren 2**.

⑪ F1 **Verbinden** drücken, um eine Verbindung mit dem hervorgehobenen Access Point herzustellen. Siehe Seite 42.

Die Verbindungsschaltfläche wird als „**Verbinden***“ angezeigt, wenn der Tester mit dem hervorgehobenen Access Point keine Verbindung herstellen kann. Siehe Seite 42.

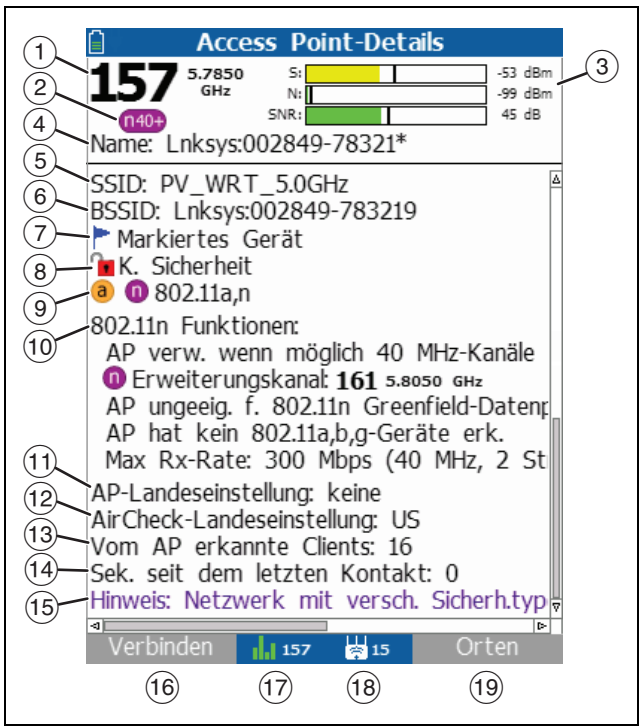
Um eine Verbindung mit einem sicheren Access Point herzustellen, benötigt der Tester ein Profil, welches Sicherheitsdaten beinhaltet. Siehe Seite 14.

⑫ 48: Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑬ 5: Die Anzahl der vom Tester am Standort wahrgenommenen Access Points. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 18.

⑭ F2 **ACL** drücken, um den Autorisierungsstatus für den hervorgehobenen Access Point zu ändern. Siehe Seite 17.

Um Details für einen Access Point anzuzeigen, den Access Point markieren und dann drücken. Siehe Abbildung 7.



gdk06.eps

Abbildung 7. Access Point-Details

(1) Der Kanal und die Frequenz des Access Points. Die Zahl ist rot, wenn Kanal für das unter **Tools** > **Land einstellen** ausgewählte Land illegal ist.

(2) n40+ n40–: Der primäre Kanal ((1)) ist mit einem Erweiterungskanal darüber (n40+) oder darunter (n40–) gebunden, wodurch ein 40 MHz-Kanal entsteht. Durch diesen breiteren Kanal wird ein höhere Durchsatz im Netzwerk möglich. Der Erweiterungskanal erscheint unter **802.11n-Funktionen** ((10)).

(3) Die Signalstärke (**S**), die Störstärke (**N**) und das Signal-Rausch-Verhältnis (**SNR**). Die Schwellenwerte für die Farben in den Balkendiagrammen können verändert werden. Die Balken sind grau, wenn der Tester den Access Point nicht wahrnehmen kann. Siehe Seite 21.

(4) **Name**: Der Name des Access Points, falls in den Beacon-Frames und Probe-Response-Frames ein Name enthalten ist.

(5) **SSID**: Service Set Identifier. Die Kennung des Netzwerks, das den Access Point verwendet.

(6) **BSSID**: Basic Service Set Identifier. Die MAC-Adresse des Access Points.

Hinweis

Einige Access Points haben unterschiedliche MAC-Adressen für die drahtgebundenen und drahtloses Schnittstellen.

⑦ Der Autorisierungsstatus des Access Points.

⑧ Der Sicherheitsstatus des Access Points.

⑨ Die 802.11-Standards, die der Access Point verwenden kann.

⑩ **802.11n-Funktionen**: Notizen für Access Points, die den 802.11n-Standard verwenden können. Siehe Tabelle 4 auf Seite 36.

⑪ **AP-Landeseinstellung:**: Der Ländercode, der vom Access Point übertragen wird. Wenn die **AP-Landeseinstellung** nicht mit der **AirCheck-Landeseinstellung** übereinstimmt, hat der Access Point rote Balken in der **802.11**-Spalte. Siehe „802.11d-Betrieb“ auf Seite 20. Anhang C enthält die Länder und die Codes.

⑫ **AirCheck-Landeseinstellung**: Der Code für das Land, das unter **Tools** > **Land einstellen** ausgewählt ist. Siehe „802.11d-Betrieb“ auf Seite 20. Anhang C enthält die Länder und die Codes.

⑬ **Vom Access Point erkannte Clients**: Die Anzahl der Clients, die derzeit den Access Point verwenden. „--“ wird angezeigt, wenn der Access Point die Anzahl seiner Clients nicht meldet.

⑭ **Sek. seit dem letzten Kontakt**: Die Anzahl der Sekunden seit der letzten Wahrnehmung des Access Points durch den Tester.

⑮ Notizen für den Access Point. Siehe Tabelle 3 auf Seite 35.

⑯ F1 **Verbinden** drücken, um eine Verbindung mit dem Access Point herzustellen. Siehe Seite 42.

Die Schaltfläche „Verbinden“ wird als „**Verbinden***“ angezeigt, wenn der Tester keine Verbindung zum markierten Netzwerk herstellen kann. Siehe Seite 42.

⑰

: Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑱

: Die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 17.

⑲ F2 **Orten** drücken, um den Access Point aufzufinden. Siehe Seite 54.

Wenn der Tester keinen Access Point erkennt

In einigen Situationen erkennt der Tester keinen Access Point:

- Der Tester kann den Access Point nicht wahrnehmen, da die Entfernung zu groß ist.
- Der Access Point sendet keine Beacons aus, wenn der Tester den Kanal überwacht, der vom Access Point verwendet wird.
- Der Tester kann den Access Point nicht wahrnehmen, da das Signal eine Wand oder ein anderes Hindernis nicht durchdringen kann.
- Der Kanal, der vom Access Point verwendet wird, ist zu stark gestört. **Kanäle** auswählen, um die Störung des Kanals durch Nicht-802.11-Quellen zu sehen.

Notizen für Netzwerke und Access Points

Die Tabellen 3 und 4 enthalten Beschreibungen für die Notizen, die der Tester zu Netzwerken und Access Points hinzufügen kann.

Tabelle 3. Notizen für Netzwerke und Access Points

Ad Hoc-Netzwerk in Betrieb	Diese SSID ist ein Ad Hoc-Netzwerk. Ein Laptop sendet die SSID aus, da der Laptop automatisch eine Verbindung zu einem anderen Laptop herstellte, der die SSID übertrug. Über Ad hoc-Geräte können sich Hacker Zugang zu Daten verschaffen, die im Netzwerk übertragen werden. (Einige IT-Richtlinien für Netzwerke lassen Ad hoc-Geräte zu.)
Kanal ist für dieses Land nicht legal	Der Access Point verwendet einen Kanal, der im unter **Tools** > **Land einstellen** ausgewählten Land nicht legal ist. Sicherstellen, dass das Land, das unter **Tools** > **Land** einstellen ausgewählt ist, korrekt ist.
Mögl. Störung - Überschneidung m. Standardkanälen	Der Access Point verwendet einen Kanal im 2,4 GHz-Band, der eine Überschneidung mit Nachbarkanälen aufweisen kann. Dies kann Störungen von benachbarten Kanälen bewirken. *Hinweis* *In den USA sind die Kanäle, die einander nicht überschneiden, die Kanäle 1, 6 und 11.*

-Fortsetzung-

Tabelle 3. Notizen für Netzwerke und Access Points (Fortsetzung)

Netzwerk mit versch. Sicherh.typen	Nicht alle Access Points für diese SSID verwenden dieselbe Sicherheitsverschlüsselung.
40 MHz 802.11n wird für 2,4 GHz nicht empfohlen	Kanäle im 2,4 GHz-Band sollten nicht gebunden werden, da dieses Band lediglich drei Kanäle aufweist, die einander nicht überschneiden. Wenn zwei Kanäle gebunden werden, ist nur noch ein Kanal für Nutzung durch andere Geräte verfügbar.
Unerwartetes Land des Access Point	Das Land des Access Points stimmt nicht mit der Einstellung im Tester unter **Tools** > **Land einstellen** überein.

Tabelle 4. 802.11n-Funktionen (angezeigt auf dem Bildschirm „Access Points-Details“)

AP verw. wenn möglich 40 MHz-Kanäle	In einigen Situationen verwendet der Access Point keine 40 MHz-Kanäle. Beispiele: • Der Access Point hat andere Access Points oder Clients wahrgenommen, die Kanäle verwenden, die eine Überschneidung mit 40 MHz-Kanälen aufweisen. • Ein Client, der den Access Point verwendet, hat derartige Access Points oder Clients wahrgenommen und den Access Point angewiesen, keine 40 MHz-Kanäle zu verwenden. Für alle Situationen, in denen Access Points keine 40 MHz-Kanäle verwenden, im 802.11n-Standard nachschlagen.
AP verwendet nur 20 MHz-Kanäle	Der Benutzer hat den Access Point so eingestellt, dass er ausschließlich 20 MHz-Kanäle verwendet.

Tabelle 4. 802.11n-Funktionen (angezeigt auf dem Bildschirm „Access Points-Details“) (Fortsetzung)

AP geeig. f.802.11n-Greenfield-Datenpkt.	Der Access Point kann die Geschwindigkeit erhöhen, wenn er Greenfield-Pakete verwendet.
AP ungeeig. f.802.11n-Greenfield-Datenpkt.	Der Access Point akzeptiert keine 802.11n-Greenfield-Packete. Der Benutzer hat den Access Point so eingestellt, dass dieser niemals Greenfield-Pakete verwendet, oder der Access Point nimmt 802.11a,b,g-Clients wahr und funktioniert nicht im Greenfield-802.11n-Modus.
AP hat 802.11a,b,g-Geräte erkannt	Der Access Point muss Schutz verwenden, sodass er keine Probleme mit a,b,g-Übertragungen verursacht. Schutzverfahren reduzieren die Geschwindigkeit des 802.11n-Netzwerks. • Der Access Point hat 802.11a,b,g-APs oder Clients wahrgenommen. • Ein Client, der Access Point verwendet, hat 802.11a,b,g-APs oder -Clients wahrgenommen.
AP hat keine 802.11a,b,g-Geräte erk.	Es ist nicht erforderlich, dass der Access Point Schutz verwendet, um Probleme mit a,b,g-Übertragungen zu vermeiden. Der Access Point kann mit maximaler Geschwindigkeit funktionieren.

-Fortsetzung-

Tabelle 4. 802.11n-Funktionen (angezeigt auf dem Bildschirm „Access Points-Details“) (Fortsetzung)

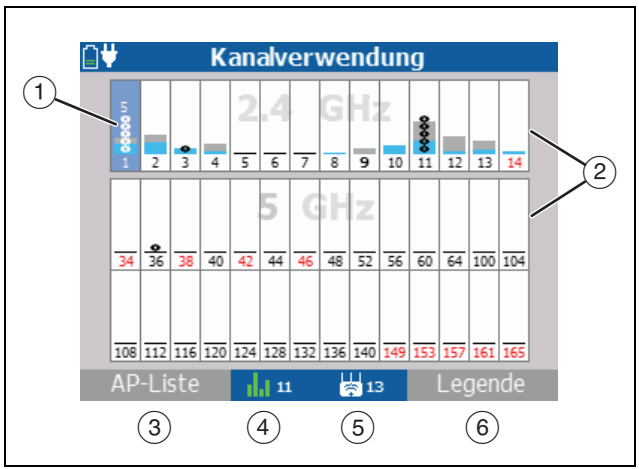
Max Rx-Rate	Die maximale Datenempfangsrate des Access Points zum aktuellen Zeitpunkt. Diese Rate kann sich ändern, wenn der Access Point Anpassungen für Änderungen beim Wireless-Verkehr im Bereich vornimmt. • **20 MHz** oder **40 MHz**: Die Kanalbreite, die erforderlich ist, um die maximale Rate zu erzielen. • **X Ströme**: Die Anzahl der Datenströme, die der Access Point verwendet, um die maximale Rate zu erzielen. • **1/2 GI**: Der Access Point verwendet ein kurzes Guard-Intervall (400 ns anstatt 800 ns), um die maximale Rate zu erzielen. Ein kurzes Guard-Interval kann zum Beispiel die Empfangsrate von 270 Mbps auf 300 Mbps erhöhen.

Kanalauslastung

Die Kanalauslastungsfunktion zeigt, wie viel Wireless-Verkehr auf den einzelnen Kanälen auftritt. Es wird auch Störungen von Nicht-802.11-Quellen angezeigt. Abbildung 8 zeigt den Bildschirm **Kanalverwendung**.

Um Details für einen Kanal anzuzeigen (Abbildung 9), verwenden, um einen Kanal zu markieren, und dann drücken.

Um die Bänder für diese Funktion auszuwählen, **Tools** auswählen und dann **802.11-Einstellungen verwalten** auswählen. Siehe Tabelle 2 auf Seite 17.



gdk08.eps

Abbildung 8. Kanalverwendung/Kanalauslastung

1. Die Balkendiagramme zeigen an, wie viel der Kanalkapazität durch 802.11-Geräte (blau) und wie viel durch Nicht-802.11-Geräte (grau) genutzt wird. Je höher der Balken ist, desto stärker ist die Auslastung des Kanals.

   Die Ringe in den Balkendiagrammen zeigen an, wie viele Access Points den Kanal verwenden. Wenn der Kanal hervorgehoben wird, wird die Anzahl der aktiven Access Points über dem Balkendiagramm angezeigt.

   Kanäle, die keine Access Points haben, können 802.11-Nutzung aufgrund von Überschneidung von Access Points auf benachbarten Kanälen anzeigen.

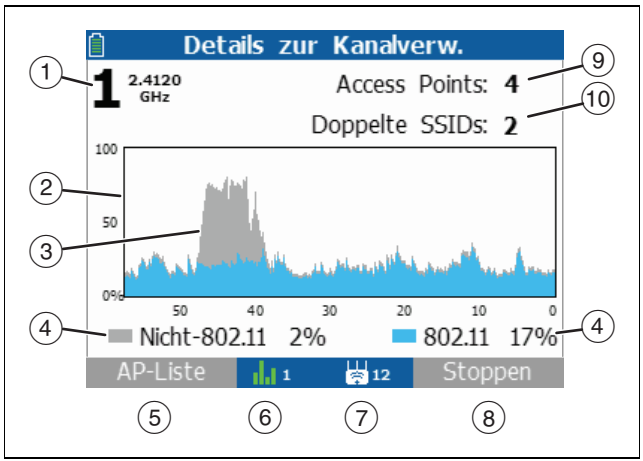
2. Der Tester zeigt standardmäßig Kanäle auf den 2,4 GHz- und 5 GHz-Bändern an. Um lediglich ein Band anzuzeigen, die Einstellung unter **Tools** > **802.11-Einstellungen verwalten** verwenden.

3. F1 **AP-Liste** drücken, um die Access Points anzuzeigen, die den hervorgehobenen Kanal verwenden.

4. 48: Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

5. 5: Die Anzahl der vom Tester am Standort wahrgenommenen Access Points. Diese Zahl entspricht der Anzahl physischer Access Points, wenn **Virtuelle Access Points gruppieren** ausgewählt ist. Siehe Seite 17.

6. Um die Beschreibungen der Symbole des Bildschirms **Kanalverwendung** anzuzeigen, F2 **Legende** drücken.



gdk09.eps

Abbildung 9. Details zur Kanalverwendung/ Kanalauslastung

(1) Die Kanalnummer und die Frequenz des Kanals, der überwacht wird. Die Zahl ist rot, wenn Kanal für das unter **Tools** > **Land einstellen** ausgewählte Land illegal ist.

Um den Kanal zu ändern, drücken.

(2) Ein Diagramm der 802.11-Auslastung und Nicht-802.11-Störung des ausgewählten Kanals im Verlauf der Zeit in Sekunden. Je höher die Kennlinie ist, desto stärker ist die Auslastung des Kanals. Sehr stark ausgelastete Kanäle können das Netzwerk verlangsamen und/oder Verbindungen beinträchtigen.

(3) Störung von einem Mikrowellenherd.

(4) **Nicht-802.11**, **802.11**: Der prozentuale Anteil der Signale auf dem Kanal: nicht von 802.11-Geräten (grau) und von 802.11-Geräten (blau).

Nicht-802.11-Störsignale können von Mikrowellenherden, Schnurlostelefonen, Bluetooth®-Geräten, Bewegungsmeldern, drahtlosen Kameras und anderen drahtlosen Geräten ausgehen. Das Störsignal kann sich auf die WLAN-Verbindung oder -Leistung auswirken.

(5) F1 **AP-Liste** drücken, um die Access Points anzuzeigen, die den Kanal verwenden. Siehe Abbildung 6.

(6) 48: Der Kanal, der vom Access Point verwendet wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Die Balken sind rot, falls der Tester unterschiedliche Ländercodes von einem oder mehreren Access Points empfangen hat. Siehe „802.11d-Betrieb“ auf Seite 20.

⑦ 5: Die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points. Diese Zahl entspricht der Anzahl physischer Access Points, wenn **Virtuelle Access Points gruppieren** ausgewählt ist. Siehe Seite 18.

⑧ F2 **Stopp** drücken, um den Bildschirm anzuhalten.

⑨ **Access Points**: Die Anzahl der Access Points, die den Kanal verwenden. Diese Zahl entspricht der Anzahl physischer Access Points, wenn **Virtuelle Access Points gruppieren** ausgewählt ist. Siehe Seite 18.

⑩ **Doppelte SSIDs**: Die Anzahl der Access Points im selben Bereich, die denselben Kanal verwenden und dasselbe Netzwerk unterstützen. Dies kann ein Problem darstellen, da die Access Points einander beeinträchtigen können.

Verbindungsprüfung

Verbindungstests verwenden, um das Funktionieren der folgenden Wireless-Netzwerkfunktionen zu prüfen.

- Clients können Verbindungen mit dem Netzwerk herstellen.
- Clients haben Zugang zu Netzwerkservices (z.B. DHCP, DNS und Router).
- Clients können mit angemessener Geschwindigkeit mit anderen Geräten kommunizieren.
- Die Reichweite für Client-Verbindungen ist zufriedenstellend.

Die Tests messen auch Leistungsparameter, die anzeigen können, ob das Netzwerk ein Problem aufweist.

Laden eines Profils, das Sicherheitsanmeldeinformationen einschließt

Der Tester muss über die richtigen Sicherheitsanmeldeinformationen verfügen, um eine Verbindung mit einem sicheren Netzwerk herzustellen. Sichere Netzwerke weisen ein grünes oder gelbes geschlossenes Schloss (🔒 🔒) in der Sicherheitsspalte auf.

Um Sicherheitsanmeldeinformationen einzugeben, AirCheck Manager verwenden, um eine Konfiguration zu erstellen, die die Anmeldeinformationen einschließt. Dann das Profil auf den Tester transferieren. Siehe Seite 14.

Hinweis

Sie können auf dem Tester keine Sicherheitsdaten erstellen oder bearbeiten. Sie können sie nur mit dem AirCheck Manager erstellen oder bearbeiten.

Laden eines Profils

1 Auf dem Startbildschirm **Tools** auswählen und dann **Dateien verwalten** auswählen.

2 **Profil laden** auswählen, das richtige Profil hervorheben, SELECT drücken und dann F2 **Laden** drücken.

Herstellen einer Verbindung mit einem Netzwerk oder Access Point

Der Tester kann eine Verbindung mit einem Netzwerk (SSID) oder mit einem bestimmten Access Point (BSSID) herstellen, um sicherzustellen, dass das Netzwerk bzw. der Access Point für Wireless-Clients verfügbar ist.

Der Tester kann auch verwendet werden, um eine Verbindung mit einem sicheren Netzwerk herzustellen und zu prüfen, dass die Sicherheitsanmeldeinformationen korrekt sind.

Der Tester zeigt die Schritte während des Verbindungsverfahrens an und erstellt ein Protokoll aufgetretener Ereignissen (Abbildungen 10 und 11).

Die Verbindungsschaltfläche wird als „**Verbinden***“ angezeigt, wenn der Tester mit dem hervorgehobenen Netzwerk oder Access Point keine Verbindung herstellen kann. Dieser Fall tritt ein, da das Netzwerk Sicherheitsanmeldeinformationen verwendet, die im Profil, das geladen wird, nicht enthalten sind.

Herstellen einer Verbindung mit einem Netzwerk

1 Falls das Netzwerk sicher ist, muss ein Konfigurationsprofil geladen werden, das die Sicherheitsanmeldeinformationen für das Netzwerk enthält. Siehe Seite 14.

2 Auf dem Startbildschirm **Netzwerke** auswählen.

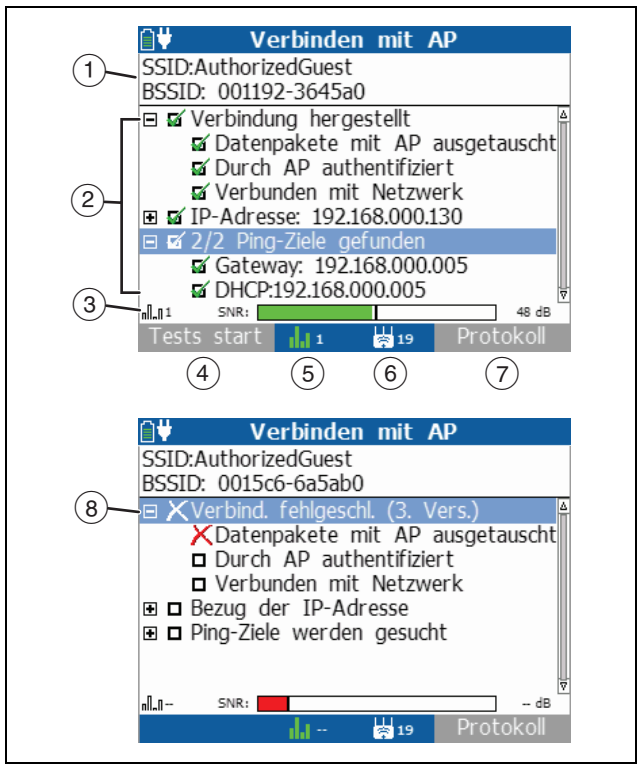
3 Das Netzwerk in der Liste **Netzwerke (SSIDs)** hervorheben und dann F1 **Verbinden** drücken.

Herstellen einer Verbindung mit einem bestimmten Access Point

1 Falls der Access Point sicher ist, muss ein Konfigurationsprofil geladen werden, das die Sicherheitsanmeldeinformationen für den Access Point enthält. Siehe Seite 14.

2 Auf dem Startbildschirm **Access Points** auswählen.

3 Den Access Point in der **Access Points**-Liste hervorheben und dann F1 **Verbinden** drücken.



gdk04.eps

Abbildung 10. Der Verbindungsbildschirm

① **SSID**, **BSSID**: Der Name des Netzwerks und die MAC-Adresse des vom Tester für die Verbindung verwendeten Access Points. Beim Herstellen einer Verbindung mit einem Netzwerk verwendet der Tester normalerweise den Access Point, der das höchste Signal-Rausch-Verhältnis (SNR) aufweist. Wenn das Netzwerk sichere und unsichere Access Points aufweist und Sicherheitsanmeldeinformationen verfügbar sind, versucht der Tester eine Verbindung mit dem sicheren Access Point herzustellen, der das höchste Signal-Rausch-Verhältnis (SNR) aufweist. Einige Netzwerke verwenden einen Controller, der eine Verbindung mit dem Access Point bereitstellt, der am wenigsten Verkehr aufweist.

② Die Schritte im Verbindungsverfahren. Die Liste für einen einzelnen Schritt wird bei Abschluss des Schritts ausgeblendet. Um die Liste für einen Schritt ein- bzw. auszublenden, den Schritt hervorheben und dann SELECT drücken.

Als Teil des Verbindungstests pingt der Tester Geräte, die die Verbindung unterstützen (z.B. die DHCP- und DNS-Server), und IP-Adressen, die im Profil enthalten sind. Der Tester zeigt ein grünes Häkchen (☑) an, falls das Gerät geantwortet hat, bzw. ein rotes X (☒), falls das Gerät nicht geantwortet hat. Um andere Geräte zu pingen, einen Ping-Test durchführen. Siehe Seite 46.

③ **SNR**: Die Kanalnummer und das Signal-Rausch-Verhältnis (SNR) für den Access Point. Die Schwellenwerte für die Farben in den Balkendiagrammen können verändert werden. Siehe Seite 21.

④ F1 **Tests starten** drücken, um einen Ping-Test durchzuführen, der den **Verbindungsreichweitentest** einschließt.

⑤ 48: Der Kanal, der vom Access Point verwendet wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑥ 5: Die Anzahl der vom Tester am Standort wahrgenommenen Access Points. Diese Zahl entspricht der Anzahl physischer Access Points, wenn **Virtuelle Access Points gruppieren** ausgewählt ist. Siehe Seite 18.

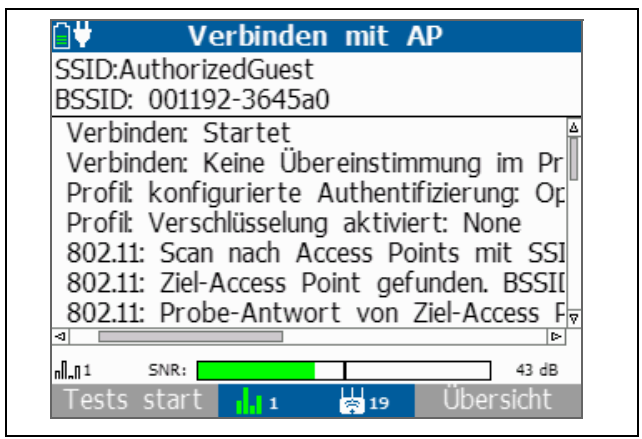
⑦ F2 **Protokoll** drücken, um Details über das Verbindungsverfahren anzuzeigen. Siehe Abbildung 11.

⑧ Eine Verbindung, die fehlgeschlagen ist. Der Tester stoppt den Verbindungsprozess nach dem dritten Versuch.

Anhang A beschreibt Protokollmeldungen, die angezeigt werden, wenn die Verbindung fehlschlägt.

Hinweis

Auf dem Verbindungsprotokollbildschirm ◂ drücken, um mit dem Bildlauf die Zeitstempel der einzelnen Protokolleinträge einzublenden. Die Zeitstempel sind in Sekunden angegeben.



gdk10.bmp

Abbildung 11. Verbindungsprotokoll

Pingen eines Geräts oder Webservers

Es können Adressen zum Pingen anderer Geräte oder Webserver eingegeben werden. Diese Funktion stellt sicher, dass andere Netzwerkgeräte verfügbar sind, und misst die Antwortzeit.

1 Eine Verbindung mit einem Netzwerk oder Access Point herstellen. Siehe Seite 42.

2 Wenn die Verbindung hergestellt ist, F1 **Tests starten** drücken.

Eine IP-Adresse aus der Liste auswählen oder eine neue Adresse eingeben.

Eingeben einer neuen Adresse

a. **IP-Adresse eingeben** auswählen.

b. Verwenden Sie ◄►, um einen Wert zum Ändern auszuwählen.

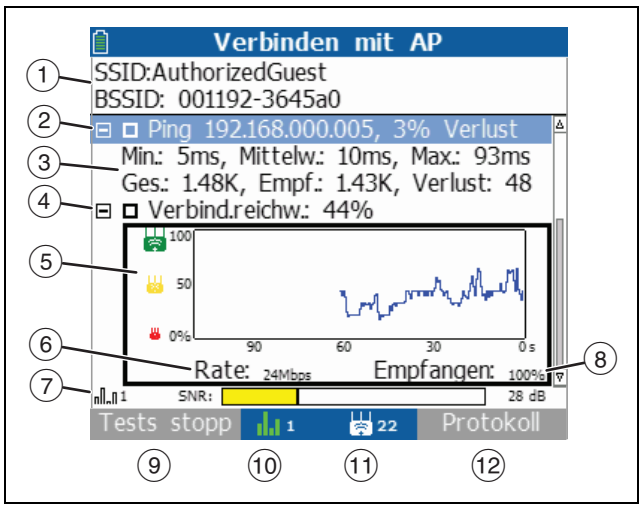
c. Verwenden Sie ▼▲, um den markierten Wert zu vergrößern bzw. zu verkleinern.

d. Um die Adresse zu speichern, F2 **Fertig** drücken.

Hinweis

Wenn das Profil gespeichert wird, speichert der Tester die eingegebenen Ping-Adressen nicht. Um die Adressen in die IP-Adressliste für Ping-Tests aufzunehmen, AirCheck Manager verwenden, um sie in ein Profil einzuschließen.

Der Ping-Bildschirm (Abbildung 12) zeigt die Ergebnisse des Ping-Tests an. Um eine andere Adresse zu pingen, F1 zweimal drücken und dann eine andere Adresse auswählen oder eingeben.



gdk21.eps

Abbildung 12. Ping-Bildschirm

1. **SSID, BSSID**: Netzwerkname und Access Point-Name für das Ping-Ziel.

2. **Pingen**: IP-Adresse für das Ping-Ziel und der prozentuale Anteil nicht empfangener Antworten.

3. Die minimalen (**Min.**), mittleren (**Mittl.**) und maximalen (**Max.**) Zeitperioden für Ping-Antworten vom Gerät und die Anzahl der während des Ping-Tests gesendeten, empfangenen und verlorenen Pakete.

4. **Verbindungsreichweite**: Die Verbindungsreichweite zeigt die Wahrscheinlichkeit der bestmöglichen Verbindung zum Access Point vom aktuellen Standort aus an. Die bestmögliche Verbindung ergibt eine Ping-Antwortrate von 100 % und die maximal mögliche Datenrate. Der Verbindungsreichweite-Wert verringert sich mit zunehmender Entfernung vom Access Point. Zuerst verringert sich die Datenrate. Mit zunehmender Entfernung vom Access Point verschlechtert sich die Ping-Antwortrate und die Verbindung wird unzuverlässig.

   Der Tester verwendet folgende Formel zur Berechnung der Verbindungsreichweite:

$$\text{Ping-Antwortrate (8)} \times \left(\frac{\text{Datenrate (6)}}{\text{Maximal mögliche Datenrate}} \right)$$

5. Ein Diagramm der Verbindungsreichweite für die letzten 120 Sekunden.

6. **Rate**: Datenübertragungsrate.

⑦ **SNR**: Die Kanalnummer des Access Points und das Signal-Rausch-Verhältnis (SNR). Die Schwellenwerte für die Farben im Balkendiagramm können verändert werden. Siehe Seite 21.

⑧ **Empfangen**: Die Ping-Antwortrate (empfangene Ping-Antworten dividiert durch gesendete Pings).

⑨ F1 **Tests stoppen** drücken, um den Ping-Test zu stoppen.

⑩ 48: Der Kanal, der vom Access Point verwendet wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑪ 5: Die Anzahl der vom Tester am Standort wahrgenommenen Access Points. Diese Zahl entspricht der Anzahl physischer Access Points, wenn **Virtuelle Access Points gruppieren** ausgewählt ist. Siehe Seite 18.

⑫ F2 **Protokoll** drücken, um Details über das Verbindungsverfahren anzuzeigen. Siehe Abbildung 11.

Ermitteln von Clients

Wenn der Tester eingeschaltet ist, überwacht er alle Kanäle auf Probe-Request-Frames von Netzwerk-Clients. Um diese Clients anzuzeigen, die Funktion **Client auflisten** verwenden. Diese Funktion zeigt, ob die Netzwerkschnittstellenkarte in einem Client Daten übertragen kann. Sie zeigt auch Informationen über den Client an, z. B. die vom Client verwendeten Kanäle, die Datenraten und die in Proben verwendeten SSIDs.

Die Client-Bildschirme enthalten die Funktion **Lokalisieren**, mit deren Hilfe Sie Clients ermitteln können.

Bei Verwendung der Funktion **Clients auflisten** überwacht der Tester alle Kanäle für eine längere Zeitdauer als bei Verwendung anderer Funktionen. Der Tester kann dadurch mehr Clients auf den einzelnen Kanälen finden.

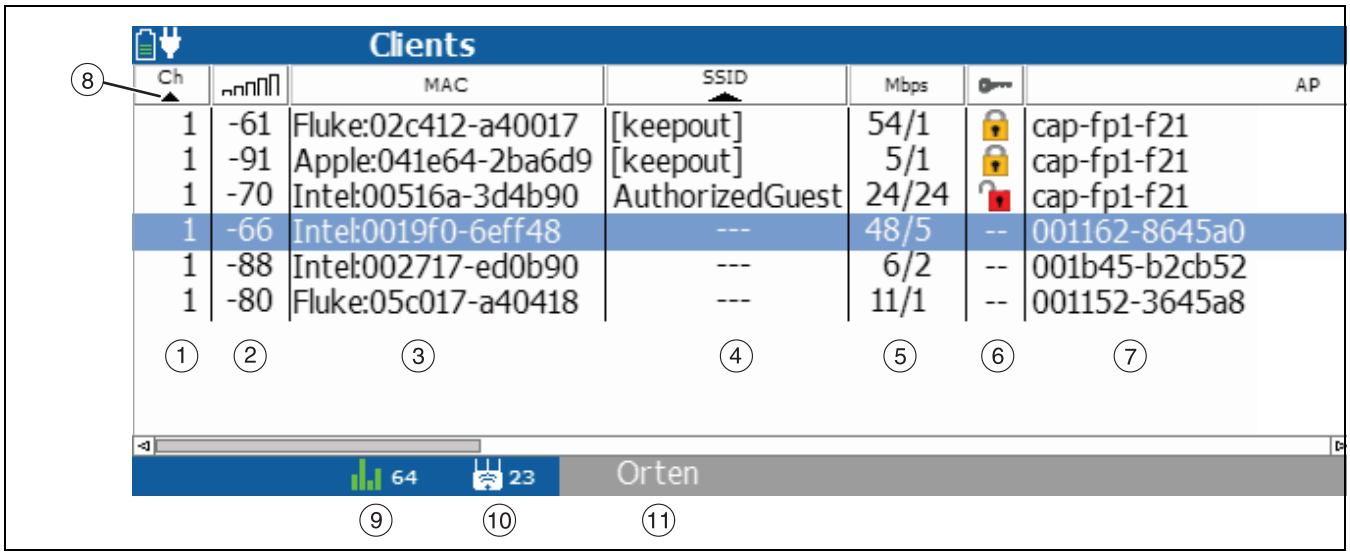
Ermitteln von Clients

Wählen Sie die Option **Tools** und anschließend die Option **Clients auflisten** aus. Abbildung 13 zeigt den Bildschirm **Clients**.

Um Details über einen Client anzuzeigen, den Client markieren und dann (SELECT) drücken. Siehe Abbildung 14.

Hinweis

Die aktuellen Informationen für einen Client werden vom Tester nur dann angezeigt, wenn der Client Daten überträgt, während der vom Client verwendete Kanal vom Tester überwacht wird. Um Client-Informationen schneller zu erfassen, wählen Sie die Optionen ***Tools*** *>* ***802.11-Einstellungen verwalten*** *aus, und aktivieren Sie nur ein Band. Dadurch wird die Anzahl der vom Tester überwachten Kanäle verringert.*



gdk12.eps

Abbildung 13. Clients-Bildschirm

① **Ch**: Der vom Client verwendete Kanal.

② : Die Stärke des Signals. Die Schwellenwerte für die Farben in den Balkendiagrammen können verändert werden. Siehe Seite 21.

③ **MAC**: Die MAC-Adresse des Clients. Die Adresse beginnt mit einem Hersteller-Abkürzungspräfix, falls der Präfix verfügbar ist. Siehe „oui_abbr.txt“ auf Seite 64.

④ **SSID**: Service Set Identifier. Der Client ist mit diesem Netzwerk verbunden.

[Unsichtbar]: Die SSID des Netzwerks wird nicht gesendet.

Wenn eine SSID in eckigen Klammern angezeigt wird, hat der Tester die unsichtbare SSID in Paketen von anderen WLAN-Clients ermittelt. In AirCheck Manager werden diese SSIDs ohne eckige Klammern angezeigt.

⑤ **Mbps**: Die Höchst- und Mindestgeschwindigkeit der Datenübertragung (in Mbit/s), die der Tester zum Zeitpunkt der letzten Überwachung des Clients festgestellt hat.

⑥ : Der Sicherheitsstatus des Access Points.

Rotes geöffnetes Schloss: Die Sicherheit ist für den Access Point nicht aktiviert.

Gelbes geschlossenes Schloss: Der Access Point verwendet das WEP-Sicherheitsprotokoll.

Grünes geschlossenes Schloss: Der Access Point verwendet ein Sicherheitsprotokoll, das sicherer ist als WEP, z. B. WPA oder WPA2.

⑦ **AP**: Der Name oder die BSSID des Access Points, der/die vom Client für die Netzwerkverbindung genutzt wird.

⑧ : **Sortieren 1**, absteigende und aufsteigende Reihenfolge

: **Sortieren 2**, absteigende und aufsteigende Reihenfolge

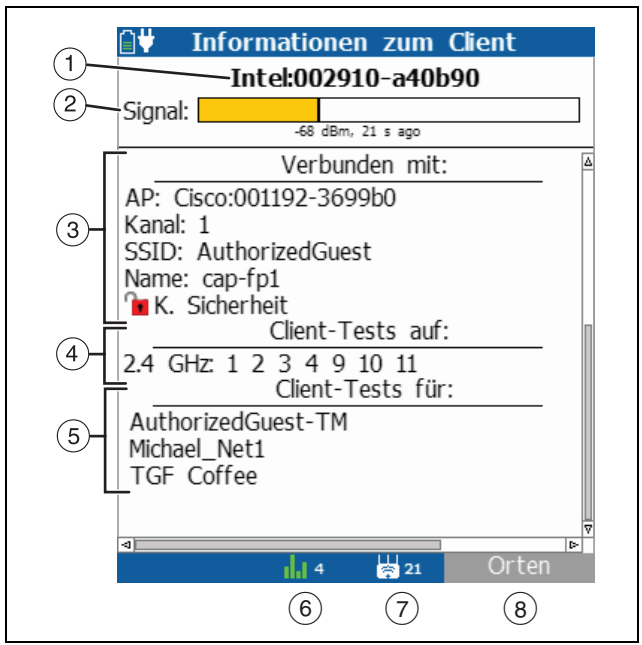
Um die Liste in aufsteigender oder absteigender Reihenfolge zu sortieren, und verwenden, um eine Spaltenüberschrift zu markieren, und dann bzw. **Sortieren 1** drücken. Um beispielsweise rasch den Access Point mit dem stärksten Signal zu finden, im Kopf der Spalte hervorheben und dann bzw. **Sortieren 1** drücken. Dadurch wird der Access Point mit dem stärksten Signal ganz oben in der Liste angezeigt.

Um in einer zweitrangigen Reihenfolge zu sortieren, markieren Sie einen anderen Spaltentitel und drücken Sie dann **Sortieren 2**.

⑨ 48: Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑩ 5: Die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 18.

⑪ F2 **Orten** drücken, um den Client zu lokalisieren. Siehe Seite 54.



gdk11.eps

Abbildung 14. Bildschirm zu Client-Details

1. Die MAC-Adresse des Clients. Die Adresse beginnt mit einem Hersteller-Abkürzungspräfix, falls der Präfix verfügbar ist. Siehe „oui_abbr.txt“ auf Seite 64.
2. **Signal**: Die Signalstärke der letzten Übertragung vom Client und die Zeitdauer seit der Wahrnehmung der Übertragung durch den Tester. Nach 120 Sekunden wechselt das Gerät auf Minuten. Nach 120 Minuten wechselt das Gerät auf Stunden.
3. **Verbunden mit**: Wenn der Client mit einem Netzwerk verbunden ist oder war oder vor Kurzem einen Verbindungsversuch unternommen hat, werden in diesem Bereich Informationen über den vom Client verwendeten Access Point angezeigt. Falls in diesem Bereich ausschließlich BSSID und der Kanal für den Access Point angezeigt werden, benötigt der Tester mehr Zeit, um Informationen zu erfassen.
4. **Client-Tests auf**: Die Kanäle, die der Client mit Tests prüft.
5. **Client-Tests für**: SSIDs, die der Client in Tests verwendet. Wenn ein Client eine Verbindung zu einem Netzwerk herstellt, wird manchmal kein Test bezüglich eines anderen Netzwerks durchgeführt, sodass die Liste nicht immer alle SSIDs umfasst, die der Client verwenden kann. Im Fall des Client-Roaming werden mehr SSIDs angezeigt.
6.

: Der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.
7.

: Die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 18.
8. F2 **Orten** drücken, um den Client zu lokalisieren. Siehe Seite 54.

Wenn der Tester keinen Client erkennt

In einigen Situationen erkennt der Tester keinen Client:

- Die Wireless-Karte im Client ist deaktiviert.
- Der Tester kann den Client nicht wahrnehmen, da die Entfernung zum Client zu groß ist.
- Der Tester kann den Client nicht wahrnehmen, da das Signal eine Wand oder ein anderes Hindernis nicht durchdringen kann.
- Der Kanal, der vom Client verwendet wird, ist zu stark gestört. **Kanäle** auswählen, um die Störung des Kanals durch Nicht-802.11-Quellen zu sehen.
- Der Tester scannt das Band nicht, das der Client verwendet. Siehe Einstellung unter **Tools** > **802.11-Einstellungen verwalten**.
- Der Client überträgt keine Probe, wenn der Tester den Kanal überwacht, der vom Client verwendet wird.

Einen Access Point oder Client lokalisieren

1 Einen Access Point lokalisieren: **Netzwerke** oder **Access Points** auswählen, dann ◁▷ und SELECT verwenden, um für den zu lokalisierenden Access Point zum Bildschirm **Access Point-Details** zu navigieren.

Einen Client lokalisieren: Wählen Sie die Option **Tools** und anschließend die Option **Clients auflisten** aus. ◁▷ verwenden, um den Client zu markieren, der lokalisiert werden soll.

2 F2 **Orten** drücken. Abbildung 15 zeigt den Bildschirm **Lokalisieren des AP**. Abbildung 16 zeigt den Bildschirm **Client lokalisieren**.

3 Den abzusuchenden Bereich in vier Abschnitte aufteilen, siehe Abbildung 17. In eine Ecke des Bereichs gehen.

4 Die Signalstärke notieren.

5 In die anderen drei Ecken des Bereichs gehen und in jeder Ecke die Signalstärke notieren.

6 In die erste Ecke des Abschnitts gehen, der das stärkste Signal aufweist.

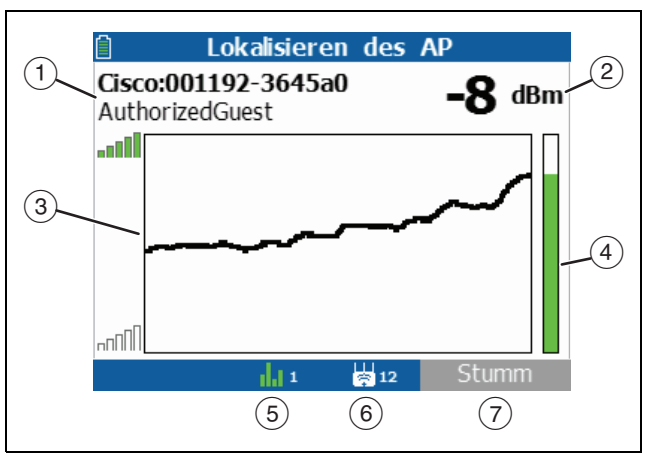
7 Die Schritte 4, 5 und 6 wiederholen, bis der Access Point oder Client gefunden ist.

Hinweiss

Falls der Access Point oder Client nicht gefunden werden kann, auf dem nächst höheren oder dem nächst tieferen Stockwerk suchen.

Wenn Sie einen Client nicht finden können und für den Client eine Verbindung mit dem Netzwerk angezeigt wird, suchen Sie zunächst nach dem Access Point, der vom Client verwendet wurde, und suchen Sie anschließend nach dem Client.

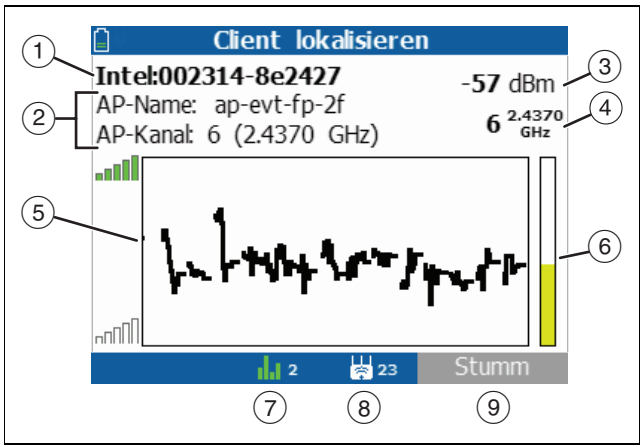
In großen offenen Bereichen kann die optionale externe Antenne nützlich sein, um Access Points schneller zu lokalisieren. Siehe Seite 58.



gdk07.eps

Abbildung 15. Lokalisieren des AP

1. Netzwerkname (SSID) und Access Point-MAC-Adresse (BSSID).
2. Die Stärke des Signals vom Access Point. Die Anzeige zeigt „**---**“ an, wenn der Tester den Access Point nicht wahrnehmen kann.
3. Ein Diagramm der Signalstärke über Zeit. Wenn der Tester den Access Point nicht wahrnehmen kann, wird die Verbindung nicht angezeigt.
4. Eine Anzeige der Signalstärke zum aktuellen Zeitpunkt. Der Balken ist grau, wenn der Tester den Access Point nicht wahrnehmen kann.
5. 48: Der Kanal, der vom Access Point verwendet wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.
6. 5: Die Anzahl der Access Points, die der Tester gefunden hat. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 17.
7. F2 **Stumm** drücken, um den Ton auszuschalten.



gdk18.eps

Abbildung 16. Bildschirm „Client lokalisieren“

① Die MAC-Adresse des Clients. Die Adresse beginnt mit einem Hersteller-Abkürzungspräfix, falls der Präfix verfügbar ist. Siehe „oui_abbr.txt“ auf Seite 64.

② Name, Kanal und Frequenz des Access Points, wie vom Client für die Netzwerkverbindung verwendet.

③ Die Stärke des Signals vom Client. Die Anzeige zeigt **„---“** an, wenn der Tester den Client nicht wahrnehmen kann.

④ Der Kanal, der vom Tester am meisten überwacht wird. Dies ist der Kanal, der vom Client verwendet wurde, als der Client das letzte Mal vom Tester wahrgenommen wurde. Der Tester überwacht diesen Kanal 2 Sekunden lang, überwacht dann einen weiteren Kanal 1 Sekunde lang und überwacht anschließend den ersten Kanal erneut 2 Sekunden lang. Wenn der Client seinen Kanal wechselt, findet der Tester den Client nach einiger Zeit auf dem neuen Kanal.

Um den Kanal zu wechseln, ◀ ▶ drücken. Der Tester überwacht den neuen Kanal 2 Sekunden lang und überwacht die anderen Kanäle weiterhin wie zuvor.

⑤ Ein Diagramm der Signalstärke über Zeit. Wenn der Tester den Client nicht wahrnehmen kann, wird die Verbindung nicht angezeigt.

⑥ Eine Anzeige der Signalstärke zum aktuellen Zeitpunkt. Der Balken ist grau, wenn der Tester den Client nicht wahrnehmen kann.

⑦ 48: Der Kanal, der vom Tester überwacht wird. Siehe ④.

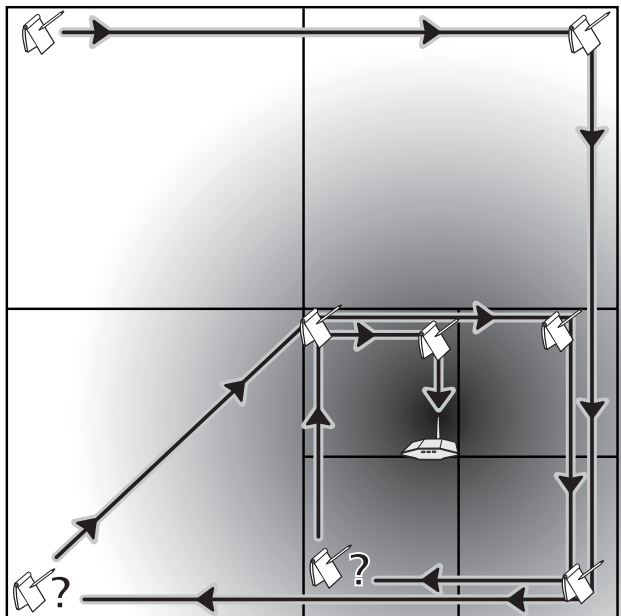
Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Siehe „802.11d-Betrieb“ auf Seite 20.

⑧ 5: Die Anzahl der Access Points, die der Tester gefunden hat. Diese Zahl schließt virtuelle Access Points nicht ein, wenn **Virtuelle Access Points gruppieren** gewählt ist. Siehe Seite 17.

⑨ F2 **Stumm** drücken, um den Ton auszuschalten.

Die Signalstärke notieren.

? In die erste Ecke des Abschnitts gehen, der das stärkste Signal verzeichnete.



ffy16.eps

Abbildung 17. Suchmuster für die Rundstrahlantenne im Tester

Der externen Richtantenne

In einem großen offenen Bereich kann die externe Richtantenne die Richtung einer Signalquelle genauer anzeigen als die im Tester integrierte Rundstrahlantenne.

Hinweis

In Bereichen, die viele Räume aufweisen (z.B. Schulen und Krankenhäuser), die interne Rundstrahlantenne verwenden, um Access Points zu lokalisieren.

Verwenden der externen Antenne zum Lokalisieren eines Access Points

1 Die Antenne an die Antennenbuchse auf der Rückseite des Testers anschließen. Der Bildschirm zeigt das Antennensymbol ( ) an, wenn die Antenne angeschlossen ist. Der Tester verwendet ausschließlich die externe Antenne, wenn eine Antenne angeschlossen ist.

Hinweis

Wenn die externe Antenne angeschlossen ist, überträgt der Tester keine Daten und stellt demzufolge keine Verbindung mit einem Netzwerk oder Access Point her.

2 Den Bereich in vier Abschnitte aufteilen, siehe Abbildung 18. In die Mitte des Bereichs gehen.

3 Einen Access Point lokalisieren: **Netzwerke** oder **Access Points** auswählen, dann ◁▷ und SELECT verwenden, um für den zu lokalisierenden Access Point zum Bildschirm **Access Point-Details** zu navigieren.

Einen Client lokalisieren: Wählen Sie die Option **Tools** und anschließend die Option **Clients auflisten** aus. ◁▷ verwenden, um den Client zu markieren, der lokalisiert werden soll.

4 F2 **Orten** drücken.

5 Die Antenne in jede Ecke des Bereichs richten. Abbildung 19 zeigt, wie die Antenne gerichtet wird.

6 In die Mitte des Abschnitts gehen, der das stärkste Signal aufweist.

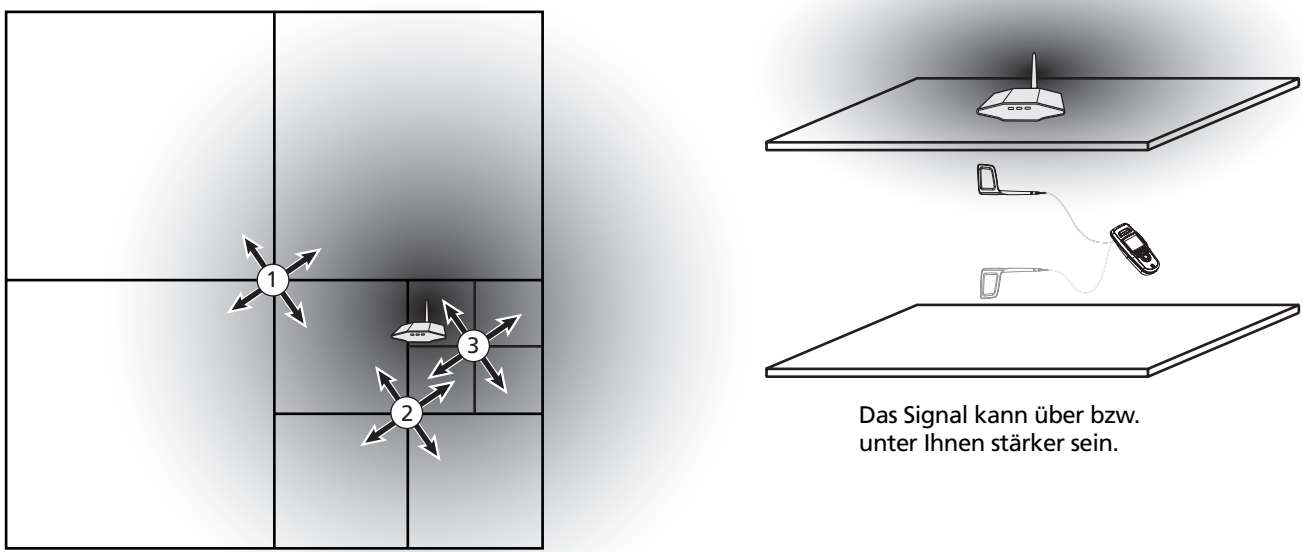
7 Die Schritte 2, 5 und 6 wiederholen, bis der Access Point oder Client gefunden ist.

Hinweis

Falls der Access Point oder Client nicht gefunden werden kann, auf dem nächst höheren und dem nächst tieferen Stockwerk suchen.

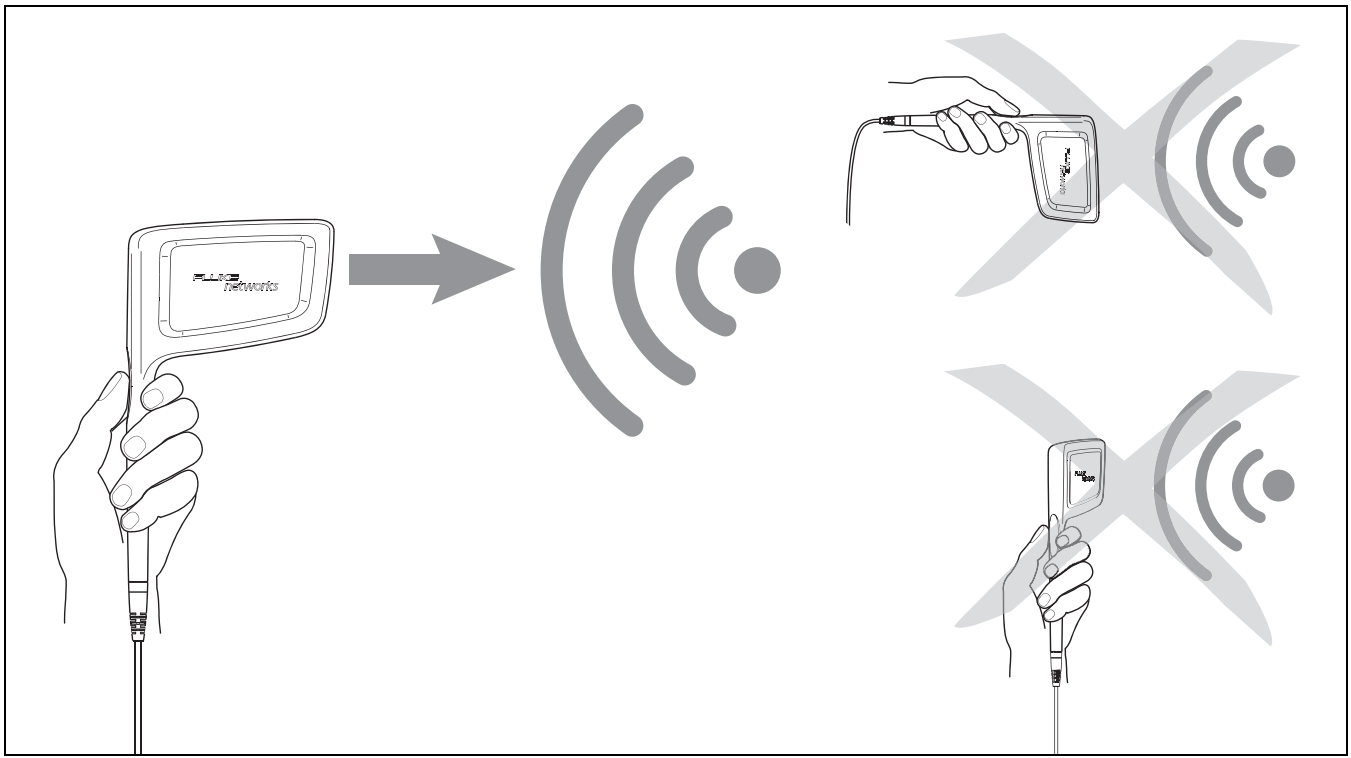
Bei Verwendung der externen Antenne diese Richtlinien verwenden:

- Die Antenne auf konstanter Höhe halten. Es können stabilere Messungen erzielt werden, wenn die Antenne höher als die Arbeitsplatzwände gehalten wird.
- Beim Drehen der Antenne in andere Richtungen, den Arm nicht bewegen. Den Tester und die Antenne in einer Position halten und den Körper drehen.


1
2
3
Das Signal kann über bzw. unter Ihnen stärker sein.
In die Mitte des Abschnitts gehen, der das stärkste Signal aufweist, bis Sie den Access Point gefunden haben.

ffy17.eps

Abbildung 18. Suchmuster für die externe Antenne



ffy13.eps

Abbildung 19. Richten der externen Antenne

Signalstärkemessungen so einstellen, dass sie mit anderen Geräten übereinstimmen

Die Signalstärkemessungen von verschiedenen Modellen von WLAN-Testern bzw. von Clients, die als Referenz verwendet werden, stimmen nicht immer miteinander überein. Die Abweichungen werden hauptsächlich durch Unterschiede bei den Antennen verursacht. Damit die Geräte übereinstimmen, können Sie einen Offset zu den AirCheck-Messungen hinzufügen.

Offset zu den Signalstärkemessungen hinzufügen

1 Offset-Wert ermitteln:

   Den AirCheck Tester und das andere Gerät verwenden, um die Signalstärke am selben Standort zu messen. Zeichnen Sie die Messabweichungen für die einzelnen Kanäle auf, um die es Ihnen geht.

2 **Tools** auswählen.

3 **802.11-Einstellungen verwalten** und dann **Benutzerdef. Signalanpassung verwenden** auswählen.

4 Im Bildschirm **Benutzer-Offsets** verwenden, um einen Kanal auszuwählen, und dann verwenden, um einen Offset-Wert auszuwählen.

5 Schritt 4 nach Bedarf für andere Kanäle wiederholen.

6 Zum Speichern der Offset-Werte F2 **Speichern** drücken.

Wenn der Tester ausgeschaltet wird, werden die Offset-Werte im Profil gespeichert. Die Offset-Werte werden auch in mit AirCheck Manager erstellten Berichten angezeigt.

⚠ Vorsicht

Damit nicht später abweichende Messungen erfolgen, denken Sie daran, dass Sie die Offset-Werte eingestellt haben.

Speichern einer Testsitzung

Die Informationen können gespeichert werden, die der Tester seit Einschaltung des Geräts, seit der letzten Speicherung einer Sitzung, seit Drücken von bzw. seit Trennung des USB-Kabels erfasst hat. Eine Sitzung umfasst die folgenden Informationen:

- Netzwerk-, Access Point-, Client- und Kanal-Informationen (ohne Diagramme)
- Eine Liste von Clients, die Proben übertragen
- Ergebnisse der Verbindung, die zuletzt hergestellt wurde
- Ergebnisse des Ping-Tests, der zuletzt durchgeführt wurde
- Das Verbindungsprotokoll

Speichern der Daten einer Testsitzung

1 drücken. Der Tester zeigt einen sequenziellen Standard-Dateinamen am unteren Rand des Bildschirms an.

- Um die Sitzung mit dem angegebenen Dateinamen zu speichern, F2 **Speichern** drücken. Der Tester speichert die Sitzung im „SESSIONS"-Ordner („SITZUNGEN"-Ordner).
- Um eine auf dem Tester gespeicherte Sitzung zu überschreiben, die Sitzung hervorheben, SELECT drücken, F2 **Speichern** drücken und dann F2 **OK** drücken.
- Um den Dateinamen zu bearbeiten, F1 **Bearbeiten** drücken.

Hinweis

Sitzungsnamen können maximal 8 Zeichen und eine Erweiterung von 3 Zeichen umfassen. Die Erweiterung muss „.ACS" lauten, wenn die Sitzung in AirCheck Manager erscheinen soll.

- Um Zeichen innerhalb des Dateinamens zu löschen, F1 **Löschen** drücken.
- Um Zeichen zum Dateinamen hinzuzufügen, verwenden um ein Zeichen hervorzuheben und dann SELECT drücken.
- Um den Cursor im Dateinamen zu verschieben, den Dateinamen hervorheben und dann drücken.
- Um die Sitzung unter dem bearbeiteten Dateinamen zu speichern, F2 **Fertig** drücken und dann F2 **Speichern** drücken.

Um die Sitzungsdatei anzuzeigen, die Datei in AirCheck Manager öffnen. Siehe Seite 65.

Verwalten von Dateien auf dem Tester

Umbenennen einer Datei

1 **Tools** auswählen und dann **Dateien verwalten** auswählen.

2 **Datei umbenennen** auswählen.

3 Eine Datei hervorheben und dann SELECT drücken.

4 Um den Dateinamen zu bearbeiten, F1 **Bearbeiten** drücken.

Hinweis

Sitzungen müssen die Erweiterung „.ACS" aufweisen und Profile die Erweiterung „.ACP", wenn sie in AirCheck Manager erscheinen sollen.

- Um Zeichen innerhalb des Dateinamens zu löschen, F1 **Löschen** drücken.
- Um Zeichen zum Dateinamen hinzuzufügen, ◀ ▶ verwenden, um ein Zeichen hervorzuheben und dann SELECT drücken.
- Um den Cursor im Dateinamen zu verschieben, den Dateinamen hervorheben und dann ◀ ▶ drücken.

5 Um die Datei unter dem bearbeiteten Namen zu speichern, F2 **Fertig** drücken und dann F2 **Umbenennen** drücken.

Löschen einer Datei

1 **Tools** auswählen und dann **Dateien verwalten** auswählen.

2 **Datei löschen** auswählen.

3 Eine Datei hervorheben und dann SELECT drücken.

4 F2 **Löschen** drücken.

Hinweis

Wenn eine Datei, die der Tester zum Betrieb benötigt, gelöscht oder umbenannt wird, erstellt der Tester beim nächsten Einschalten die Datei neu. Dies gilt nicht für erstellte Profile, gespeicherte Sitzungsdateien und die Datei OUI_ABBR.TXT. *Siehe „Dateien auf dem Tester" auf Seite 64".*

Anzeigen des verfügbaren Speicherplatzes

Das gelieferte USB-Kabel verwenden, um den Tester am PC anzuschließen, und dann eines der folgenden Verfahren verwenden:

- AirCheck Manager starten, **Tools** > **Profil-Manager** auswählen und dann das Diagramm **Speicher genutzt** ansehen.
- Den Dateibrowser des PC-Betriebssystems verwenden, um zu sehen, wie viel Speicherplatz auf dem Tester verfügbar ist.

Wenn der Speicher voll ist, zeigt der Tester beim Versuch, eine Messung zu speichern, **Speicher voll** an.

Dateien auf dem Tester

Der Tester speichert Daten im XML-Format (Extensible Markup Language). Die Daten in XML-Dateien enthalten Identifizierungs-Tags. Diese Tags können durch Software gelesen und die Daten können entsprechend interpretiert werden. Beispielsweise kann ein Webbrowser die Tags lesen und XML-Dateien auf einer Webseite anzeigen.

Der Tester erstellt folgende Typen von XML-Dateien (Standarddateiname):

- DEVICE.XML: Diese Datei enthält die Informationen, die unter **Tools** > **AirCheck-Informationen anzeigen** angezeigt werden.
- CURRENT.ACP: Diese Datei enthält eine Kopie des aktuellen Profils. Die Datei enthält auch Änderungen, die an den Einstellungen vorgenommen wurden, seitdem das Profil gespeichert/geladen wurde.
- SNXXXXXX.ACS: Sitzungsdateien enthalten Informationen über Wireless-Netzwerke. Siehe „Einen Access Point oder Client lokalisieren“ auf Seite 54“. AirCheck Manager verwendet Sitzungsdateien, um Sitzungsberichte zu erstellen.

Die Textdatei OUI_ABBR.TXT enthält Abkürzungen für die Namen von Herstellern, die Schnittstellengeräte für Netzwerke herstellen. Der Tester verwendet die Abkürzungen als Präfixe für MAC-Adressen.

Laden der neuesten Liste von Herstellerpräfixen in den Tester

1. Die neueste Version von AirCheck Manager auf dem PC starten und dann den Tester an den PC anschließen.
2. **AirCheck** > **Software aktualisieren** auswählen und dann die Registerkarte **Hersteller-MAC-Präfixdatei** auswählen.

3 Auf **Aktualisieren von Datei** klicken, die Präfixdatei (oui_abbr.txt) auswählen und dann auf **Öffnen** klicken.

Falls es auf der Fluke Networks-Website eine neuere Liste gibt, die nicht in der neuesten Version von AirCheck Manager enthalten ist, die Datei in den Herstellerpräfix-Ordner für AirCheck Manager kopieren. Dann die obigen Schritte ausführen, um die Liste in den Tester zu laden.

Transferieren von Dateien auf einen PC

Verwenden von AirCheck Manager, um auf dem Tester gespeicherte Testsitzungen oder Profile einzusehen

1 Die neueste Version der AirCheck Manager-Software auf dem PC installieren. Die Software starten.

2 Den Tester einschalten.

3 Das gelieferte USB-Kabel verwenden, um den Tester am PC anzuschließen. Der AirCheck-Bereich zeigt Sitzungsdateien an, die sich auf dem Tester befinden.

Um die Profile anzuzeigen, die sich auf dem Tester befinden, auf der AirCheck Manager-Symbolleiste **Tools** > **Profil-Manager** auswählen.

Verwenden des PC-Betriebssystems zum Übertragen von Dateien

1 Den Tester einschalten.

2 Das gelieferte USB-Kabel verwenden, um den Tester am PC anzuschließen. Das PC-Betriebssystem zeigt den Tester als Laufwerk an.

3 Das PC-Betriebssystem verwenden, um Dateien vom Tester auf ein Laufwerk des PCs zu kopieren.

Wartung

⚠Warnung⚠

Zur Vermeidung von Feuer, Stromschlag, Verletzungen oder Beschädigungen des Testers folgende Richtlinien einhalten:

- **Das Gehäuse nicht öffnen. Es können keine Teile im Innern des Gehäuses repariert oder ersetzt werden.**
- **Nur Ersatzteile verwenden, die von Fluke Networks genehmigt sind.**

- **Falls Teile ersetzt werden, die nicht als ersetzbare Teile spezifiziert sind, gilt die Garantie nicht für das Produkt und die Verwendung des das Produkt ist u. U. gefährlich.**
- **Nur Servicezentren verwenden, die von Fluke Networks genehmigt sind.**

Reinigen des Testers

Um die Anzeige zu reinigen, Linsenreiniger und ein weiches, fusselfreies Tuch verwenden. Um das Gehäuse zu reinigen, ein weiches, leicht mit Wasser oder mit Wasser und einem milden Reinigungsmittel angefeuchtetes Tuch verwenden.

⚠Vorsicht

Um Beschädigung der Anzeige oder des Gehäuses zu vermeiden, keine Lösungsmittel und keine scheuernden Materialien verwenden.

Aktualisieren der Software im Tester

1. Laden Sie die AirCheck-Aktualisierungsdatei von der Website von Fluke Networks herunter, oder wenden Sie sich an Fluke Networks, um die Aktualisierung anderweitig anzufordern. Speichern Sie die Datei auf der Festplatte.
2. Beziehen Sie die neueste Version von AirCheck Manager über die Fluke Networks-Website.
3. AirCheck Manager auf dem PC starten.
4. Den Tester einschalten.
5. Das gelieferte USB-Kabel verwenden, um den Tester am PC anzuschließen.
6. In AirCheck Manager **AirCheck** > **Software aktualisieren** auswählen.
7. Auf **Auswählen** klicken und die Aktualisierungsdatei (Erweiterung .xlf) finden und dann auf **Öffnen** klicken.
8. Auf **Aktualisieren** klicken.
9. Wenn die Übertragung fertig ist, das USB-Kabel vom Tester trennen.

10 Der Bildschirm am Tester ist leer und der Tester tickt während der Installation der Aktualisierungsdatei. Wenn die Aktualisierung fertig ist, wird auf dem Tester der Startbildschirm eingeblendet.

Hinweis

Die Ein-/Aus-Taste ist während einer Softwareaktualisierung deaktiviert. Wenn die Batterie entfernt wird, bevor die Aktualisierung abgeschlossen ist, startet die Aktualisierung bei Einschaltung des Testers erneut.

Werkseitige Standardeinstellungen wiederherstellen

Anhang B enthält eine Liste der Standardeinstellungen für den Tester.

Wiederherstellen der Standardeinstellungen

1 Auf dem Startbildschirm **Tools** auswählen, **Werkseit. Standardeinst. wiederherst.** auswählen und dann F2 **OK** drücken.

2 Um den Vorgang abzuschließen, SELECT drücken und dann den Tester einschalten.

Gerätinformationen

Anzeigen von Informationen über den Tester

Auf dem Startbildschirm **Tools** auswählen und dann **AirCheck-Informationen anzeigen** auswählen.

- **Seriennummer**: Die Seriennummer ist auch unter dem Batteriepack angegeben.
- **MAC-Adresse**: Media Access Control-Adresse. Die eindeutige Adresse des Testers.
- **SW-Version**: Die Version der Software im Tester.
- **USB-Version**: Die Version des USB-Treibers im Tester.
- **Funkversion**: Die Version des Funkgeräts im Tester.

Wenn der Tester nicht ausschaltet

Wenn der Tester nicht ausschaltet, ⏻ ca. 5 Sekunden lang gedrückt halten.

Wenn der Tester nach wie vor nicht ausschaltet, das Batteriepack entfernen und dann wieder einsetzen.

Optionen und Zubehör

Tabelle 5 listet verfügbare Optionen und Zubehör für den AirCheck Wi-Fi Tester.

Zum Anzeigen einer kompletten Liste von Optionen und Zubehör siehe die Fluke Networks-Website unter **www.flukenetworks.com/de**.

Tabelle 5. Optionen und Zubehör

Option oder Zubehör	Fluke Networks Modellnummer
Externe Richtantenne mit RSMA-Steckverbinder	EXTANT-RPSMA
Lithium-Ion-Batteriepack für den AirCheck Tester	WBP-LION
Power over Ethernet-Detektor	POE-DETECTOR
Adapter/Ladegerät für Anschluss an einen Kfz-Zigarettenanzünder	MS-Auto-Chg
Netzadapter/Ladegerät, universal, 120-240 V Wechselspannung	DTX-ACUN

Spezifikationen

Umweltspezifikationen

Betriebstemperatur und relative Luftfeuchtigkeit	32 °F bis 113 °F (0 °C bis +45 °C) *Hinweis* *Die Batterie wird nicht aufgeladen, wenn die Innentemperatur des Testers 45 °C übersteigt.*
Relative Luftfeuchtigkeit bei Betrieb (% RL, nicht kondensierend)	90 % (50 °F bis 95 °F; 10 °C bis 35 °C) 75 % (95 °F bis 113 °F; 35 °C bis 45 °C)
Lagertemperatur	-4 °F bis 140 °F (-20 °C bis +60 °C)
Stoß- und Vibrationsfestigkeit	Statistisch, 2 g, 5 Hz bis 500 Hz (Klasse 2), 1-m-Falltest
Sicherheit	EN 61010-1 2. Ausgabe
Höhenlage	4.000 m; Lagerung: 12.000 m
EMV	FCC Teil 15, Klasse A, EN 61326-1

Zertifizierung und Übereinstimmung	CE Übereinstimmung mit den relevanten Richtlinien der Europäischen Union
	N10140 Übereinstimmung mit den relevanten australischen Standards
	C SA US Aufgeführt durch die Canadian Standards Association
	FC Übereinstimmung mit den FCC-Richtlinien, Teile 15.107, 15.109
	ANATEL 1572-10-5988 (01)07898941652029 Zertifiziert durch die National Agency of Telecommunications (Anatel)

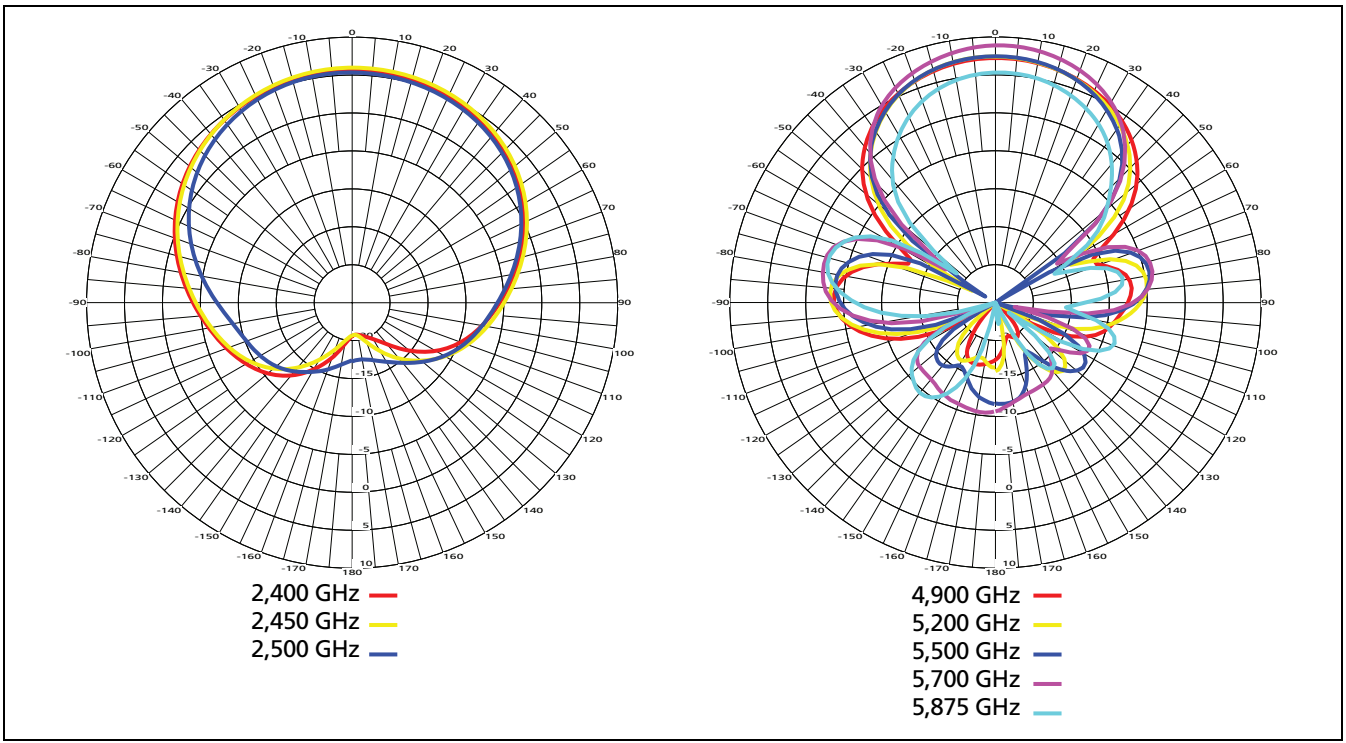
Allgemeine Spezifikationen

Abmessungen	8,89 cm x 19,81 cm x 4,83 cm
Gewicht	0,4 kg
Batterie	Entfernbares/wiederaufladbares Li-Ion-Batteriepack (18,5 Wh)
Batterielebensdauer	Typische Betriebsdauer: 5,5 Stunden. Typische Aufladezeit: 3 Stunden
Netzadapter/Batterieladegerät, extern	Wechselstromeingang 90 bis 264 VAC 48 bis 62 Hz Eingangsleistung Gleichstromausgang 15 VDC bei 1,2 A
Anzeige	2,8 Zoll LCD-Farbanzeige (320 x 240 Pixel)
Tastenfeld	12 Tasten, elastisch
LEDs	2 LEDs (Sende- und Link-Anzeige)
Host-Schnittstelle	USB Mini-B, 5-polig
Wireless-Antenne	Intern
Anschluss für externe Antenne	Nur Eingang. SMA-Steckverbinder, umgekehrte Polarität.

Wireless-Spezifikationen

Spezifikationsübereinstimmung	IEEE 802.11a, 11b, 11g, 11n
Betriebsfrequenzen *Hinweis* *Hierbei handelt es sich um die Mittenfrequenzen der Kanäle, die vom AirCheck Tester unterstützt werden.*	**Empfangene Kanalfrequenzen** *Hinweis* *Der Tester kann in jedem Land über alle Frequenzen Signale empfangen.* 2,4 GHz-Band: 2,412 GHz bis 2,484 GHz (Übertragungskanal 1 bis 14) 5 GHz-Band: 5,170 GHz bis 5,320 GHz, 5,500 GHz bis 5,700 GHz, 5,745 GHz bis 5,825 GHz (Übertragungskanäle 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165) **Kanalfrequenzen zur Übertragung** *Hinweis* *Der Tester überträgt Signale nur über die im jeweiligen Land zulässigen Frequenzen.* **2,4 GHz-Band** 802.11b: 2,412 GHz bis 2,484 GHz (Übertragungskanal 1 bis 14) 802.11g/n 20 MHz BW (HT20): 2,412 GHz bis 2,472 GHz (Übertragungskanal 1 bis 13) 802.11n 40 MHz BW (HT40): 2,422 GHz bis 2,462 GHz (inklusive aller legal verbundenen Übertragungskanal-Kombinationen)

	Kanalfrequenzen zur Übertragung (Fortsetzung) **5 GHz-Band** 802.11a/n 20 MHz BW (HT20): 5,180 GHz bis 5,320 GHz, 5,500 GHz bis 5,700 GHz, 5,745 GHz bis 5,825 GHz (Übertragungskanäle 36, 40, 44, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165) 802.11n 40 MHz BW (HT40): 5,190 GHz bis 5,310 GHz, 5,510 GHz bis 5,670 GHz, 5,755 GHz bis 5,795 GHz (inklusive aller legal verbundenen Übertragungskanal-Kombinationen)
Regulatorische Domäne	Weltmodus, 802.11d-konform
Externe Richtantenne	
Frequenzen	Frequenzbereich: 2,4 GHz bis 2,5 GHz und 4,9 GHz bis 5,9 GHz Minimaler Gewinn: 5,0 dBi im 2,4 GHz-Band und 7,0 dBi im 5 GHz-Band
Anschluss	SMA-Stecker, umgekehrte Polarität



ffy20.eps

Abbildung 20. Antennenmuster für die externe Antenne (Magnitude (dBi)) vs. Azimut (Grad)

Erklärung zu Störaussendungen – FCC (Federal Communication Commission) und IC (Industry Canada)

Diese Ausrüstung wurde getestet und stimmt mit den Grenzwerten für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC- und IC-Richtlinien überein. Diese Grenzwerte bieten angemessenen Schutz vor unerwünschten Störungen beim Betrieb des Geräts in einer Wohnumgebung. Dieses Gerät erzeugt und verwendet Funkfrequenzenergie und strahlt diese möglicherweise ab. Wenn das Gerät nicht in Übereinstimmung mit den Anweisungen installiert und betrieben wird, kann die Funkfrequenzenergie die Funkkommunikation durch unerwünschte Störungen beeinträchtigen. Es gibt jedoch keine Garantie, dass in einer bestimmten Installation keine Störungen auftreten. Falls dieses Gerät unerwünschte Störungen für Radio- oder Fernsehempfang verursacht (was durch Ein- und Ausschalten des Geräts festgestellt werden kann), wird dem Benutzer empfohlen, die Störung mit einer der folgenden Maßnahmen zu korrigieren:

- Die Empfangsantenne neu ausrichten bzw. neu platzieren.
- Den Abstand zwischen dem Gerät und dem Empfänger vergrößern.
- Das Gerät an eine Steckdose eines Schaltkreises anschließen, der sich von dem Schaltkreis unterscheidet, an dem der Empfänger angeschlossen ist.
- Für Unterstützung den Händler oder einen erfahrenden Radio-/Fernsehtechniker anfragen.

FCC-Vorsichtshinweis: Jegliche Änderungen oder Modifikationen, die von der für die Übereinstimmung verantwortlichen Partei nicht ausdrücklich genehmigt wurden, können die Befugnis zum Betrieb dieses Geräts nichtig machen.

Dieses Gerät stimmt mit Teil 15 der FCC- und IC-Richtlinien überein. Der Betrieb unterliegt den folgenden zwei Bedingungen:

(1) Dieses Gerät darf keine unerwünschten Störungen verursachen, und (2) dieses Gerät muss alle empfangenen Störungen akzeptieren, einschließlich Störungen, die u. U. unerwünschte Wirkungen verursachen.

Wichtiger Hinweis: Erklärung zur Strahlenbelastung – FCC und IC

Diese Ausrüstung stimmt mit den für eine unkontrollierte Umgebung festgesetzten FCC- und IC-Strahlenbelastungsgrenzwerten überein. Diese Ausrüstung muss unter Einhaltung eines Mindestabstands von 20 cm zwischen Strahler und Körper des Installateurs installiert und betrieben werden.

Dieser Sender darf nicht zusammen mit einer anderen Antenne oder einem anderen Sender aufgestellt oder betrieben werden.

Betrieb im 5,15 GHz- bis 5,25 GHz-Band ist auf Verwendung in Gebäuden eingeschränkt.

Die Verfügbarkeit spezifischer Kanäle und/oder Betriebsfrequenzbänder sind vom Land abhängig und für den Endbenutzer nicht zugänglich.

Europa-EU Konformitätserklärung

Dieses Gerät stimmt mit den wesentlichen Anforderungen der R&TTE Richtlinie 1999/5/EC überein. Die folgenden Testmethoden wurden angewendet, um Vermutung von Konformität mit den wesentlichen Anforderungen der R&TTE Richtlinie 1999/5/EC zu überprüfen:

- **EN60950-1: 2001 A11: 2004**

  Sicherheit von IT-Ausrüstung

- **EN50385: (2002-08)**

  Produktstandard zum Nachweis der Übereinstimmung von Funk-Basisstationen und stationären Datenstationen für Wireless-Telekommunikationssysteme mit den Grundeinschränkungen bzw. den Referenzpegeln in Bezug auf menschliche Exposition gegenüber elektromagnetischen Funkfrequenzfeldern (110 MHz bis 40 GHz) - Allgemeine Öffentlichkeit.

- **EN 300328 V1.7.1: (2006-10)**

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM); Breitband-Übertragungssysteme; Datenübertragungsgeräte, die im 2,4 GHz-ISM-Band arbeiten und Breitband-Modulationstechniken verwenden; harmonisierte EN, die wesentliche Anforderungen nach Artikel 3.2 der R&TTE-Richtlinie enthält.

- **EN 301 893 V1.4.1: (2007-07)**

  Breitband-Funkzugangsnetze (BRAN); 5 GHz-Hochleistungs-RLAN; harmonisierte EN, die wesentliche Anforderungen nach Artikel 3.2 der R&TTE-Richtlinie enthält.

- **EN 301 489-1 V1.6.1: (2005-09)**

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM); Elektromagnetische Verträglichkeit (EMV) – Standard für Funkausrüstung und -dienste; Teil 1: Allgemeine technische Anforderungen

- **EN 301 489-17 V1.2.1: (2002-08)**

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM); Elektromagnetische Verträglichkeit (EMV) – Standard für Funkausrüstung und -dienste; Teil 17: Spezifische Bedingungen für 2,4 GHz-Breitband-Übertragungssysteme und 5 GHz-Hochleistungs-RLAN-Ausrüstung.

Dieses Gerät ist ein 2,4 GHz-Breitband-Übertragungssystem (Transceiver), ausgelegt für Gebrauch in allen EU-Mitgliedstaaten und EFTA-Ländern, ausgenommen Frankreich und Italien, wo eingeschränkte Nutzung gilt.

In Italien muss der Endbenutzer eine Lizenz bei der für das Funkspektrum zuständigen Behörde beantragen, um die Befugnis zur Verwendung des Geräts zur Errichtung von Funkverbindungen im Freien und/oder zur Bereitstellung von öffentlichem Zugang zu Telekommunikations- und/oder Netzwerkdiensten zu erhalten.

Dieses Gerät darf in Frankreich nicht zur Errichtung von Funkverbindungen im Freien verwendet werden, und in bestimmten Gebieten kann die HF-Ausgangsleistung auf 10 mW EIRP im Frequenzbereich von 2454 MHz bis 2483,5 MHz begrenzt sein. Für ausführliche Informationen sollte sich der Endbenutzer an die für das Funkspektrum zuständige Behörde in Frankreich wenden.

Anhang A: Protokollmeldungen für fehlgeschlagene Verbindungen

Das Verbindungsprotokoll (Seite 45) erklärt u. U., warum ein Gerät keine Verbindung mit dem Netzwerk herstellen kann. Dieser Anhang enthält Ursachen für Protokollmeldungen, die angezeigt werden, wenn eine Verbindung fehlschlägt.

Meldung	Mögliche Ursachen für Verbindungsfehler
802.11: Keine Access Pointss gefunden	Der Access Point liegt außerhalb der Reichweite, oder das Frequenzband wurde verändert.
802.11: Warnung: AP mit SSID gefunden, Sicherheitskonfig. stimmen nicht überein	Der Tester verfügt nicht über die korrekten Typen von 802.1X-Authentifizierung/Verschlüsselung.

Meldung	Mögliche Ursachen für Verbindungsfehler
Authentifizierung fehlgeschlagen	Die Zugriffskontrollliste und der MAC-Filter auf dem Access Point haben die MAC-Adresse des Tester zurückgewiesen. Der Access Point verwendet WEP-Sicherheit, und die Low-Level 802.11-Authentifizierung (open/shared), die der Tester verwendet, unterscheidet sich vom Authentifizierungstyp, den der Access Point verwendet.
802.11: Deauthentifizierungs-Datenpaket empfangen	Wenn diese Meldung auf die Meldung **802.1X: EAP-4-Weg-Schlüssel mit Client-Nonce und Info-Elementen werden gesendet** folgt, wird sie häufig durch einen inkorrekt vorinstallierten Schlüssel (passphrase) verursacht.
Verbinden: Fehlschlagen der automatischen PAC-Beschaffung (Phase 0) erwartet	Der Tester zeigt diese Meldung immer an, wenn er mit EAP-FAST-Authentifizierung versucht eine Verbindung mit einem Access Point herzustellen. Es sind mehrere Phasen für eine EAP-FAST-Verbindung erforderlich, und Fehler treten gewöhnlich in der anfänglichen Phase auf.

Meldung	Mögliche Ursachen für Verbindungsfehler
802.1X: EAP-Fehler empfangen	• Wenn diese Meldung auf die Meldung **802.1X TLS: Client-Schlüsselaustausch wird gesendet** folgt, wird sie häufig durch ein inkorrektes Client-Zertifikat verursacht. • Wenn diese Meldung auf die Meldung **802.1X EAP-MSCHAPv2: Antwortet auf die Herausforderung** folgt, wird sie häufig durch einen inkorrekten Benutzernamen oder ein inkorrektes Kennwort verursacht. • Wenn diese Meldung auf die Meldung **802.1X: NAK** folgt, tritt sie häufig auf, weil der RADIUS-Server den EAP-Typ nicht unterstützt.
802.1X: Serverzertifikat nicht verifiziert	Diese Meldung ignorieren, falls die Option **Serverzertifikat prüfen** im Profil in AirCheck Manager nicht ausgewählt wurde.
802.1X: Serverzertifikat ist ungültig	Die Option **Serverzertifikat prüfen** wurde im Profil in AirCheck Manager ausgewählt, aber es wurde ein inkorrektes Zertifikat in den Tester geladen.

Meldung	Mögliche Ursachen für Verbindungsfehler
DHCP: Timeout aufgetreten (ohne die Meldung **DHCP: Erfolg** nach diesem)	• Der Access Point konnte nicht mit dem externen DHCP-Server kommunizieren. • Der Access Point verfügt über einen internen DHCP-Server, der jedoch deaktiviert ist. • Der DHCP-Server hat hinsichtlich der Anzahl der Benutzer seine Grenze erreicht. • Der Tester und der Access Point sind beide für WEP-Sicherheit konfiguriert, weisen jedoch unterschiedliche Schlüsseleinstellungen auf.
DHCP: Kein Angebot empfangen	Wenn diese Meldung auf die Meldung **DHCP: Timeout aufgetreten** folgt, die obigen Ursachen in Betracht ziehen.
Statisch: ARP empfangen. Adresse bereits verwendet.	Die Option **Manuell (statisch)** wurde im Profil in AirCheck Manager ausgewählt, aber es wurde eine doppelte IP-Adresse in Netzwerk gefunden.

Anhang B: Standardeinstellungen

Dieser Anhang enthält die Standardeinstellungen für den Tester, **wenn Tools > Werkseit. > Standardeinst. wiederherst.** ausgewählt wird.

Funktion	Standard-einstellung
Profil, das der Tester verwendet	Default
Automatische Ausschaltung	Ein
Sprache	Die Sprache, die zuletzt ausgewählt wurde
Land	USA
Audio für die AP-Ortungsfunktion	Ein

Funktion	Standard-einstellung
Schwellenwerte für Balkendiagramme	
Signalstärke: Rot	-80 dBm
Signalstärke: Gelb	-60 dBm
Signalstärke: Grün	-45 dBm
Störungsgrad: Rot	-60 dBm
Störungsgrad: Gelb	-80 dBm
Störungsgrad: Grün	-90 dBm
Serien-Nr. Level Rot	20 dB
Serien-Nr. Level Gelb	30 dB
Serien-Nr. Level Grün	40 dB

Funktion	Standard-einstellung
802.11-Einstellungen	
Bänder	2,4 GHz und 5 GHz
Proben übertragen	Aktivieren
Virtuelle Access Points gruppieren	Aktivieren
„Nicht hörbare APs ausgrauen“ oder „Nicht hörbare APs löschen“	Nicht hörbare APs ausgrauen
Benutzer-Offsets für benutzerdefinierte Signalanpassungen	0 dB
Netzwerkliste (SSIDs)	
Sortieren 1	SSID
Sortieren 2	SSID
Individuelle Netzwerke	
Sortieren 1	Name/MAC
Sortieren 2	Name/MAC

Funktion	Standard-einstellung
Access Points auf einem Kanal	
Sortieren 1	Name/MAC
Sortieren 2	Name/MAC
Access Points-Liste	
Sortieren 1	Name/MAC
Sortieren 2	Name/MAC
Liste der virtuellen Access Points	
Sortieren 1	SSID
Sortieren 2	SSID
Clients-Liste	
Sortieren 1	MAC
Sortieren 2	Kanal

Anhang C: 802.11d-Ländercodes

Dieser Anhang enthält die Ländercodes, die der Tester auf dem Bildschirm **Access Point-Details** anzeigt.

Länder, die fett formatiert sind, können unter **Tools** > **Land einstellen** ausgewählt werden.

Hinweis

Der Tester kann die Ländercodes mit einem dritten Zeichen anzeigen. Dieses Zeichen kann beim Suchern des Ländercodes in der nachfolgenden Tabelle ignoriert werden.

AD	Andorra
AE	**Vereinigte Arabische Emirate**
AF	Afghanistan
AG	Antigua und Barbuda
AI	Anguilla
AL	**Albanien**
AM	**Armenien**
AN	**Niederländische Antillen**
AO	Angola
AQ	Antarktis
AR	**Argentinien**

AS	Amerikanisch-Samoa
AT	**Österreich**
AU	**Australien**
AW	Aruba
AX	Aland
AZ	**Aserbaidschan**
BA	**Bosnien und Herzegowina**
BB	Barbados
BD	**Bangladesch**
BE	**Belgien**
BF	Burkina Faso
BG	**Bulgarien**
BH	**Bahrain**
BI	Burundi
BJ	Benin
BL	Sankt Bartholomäus
BM	Bermuda

BN	**Brunei Darussalam**
BO	**Bolivien**
BR	**Brasilien**
BS	Bahamas
BT	Bhutan
BU	Burma (transitional)
BV	Bouvetinsel
BW	Botswana
BY	**Weißrussland**
BZ	**Belize**
CA	**Kanada**
CC	Kokosinseln
CD	Kongo, Demokratische Republik
CF	Zentralafrikanische Republik
CG	Kongo
CH	**Schweiz**
CI	Elfenbeinküste

CK	Cookinseln
CL	**Chile**
CM	Kamerun
CN	**China**
CO	**Kolumbien**
CR	**Costa Rica**
CS	**Serbien und Montenegro (transitional)**
CU	Kuba
CV	Kap Verde
CX	Weihnachtsinsel
CY	**Zypern**
CZ	**Tschechien**
DE	**Deutschland**
DJ	Djibouti
DK	**Dänemark**
DM	Dominica
DO	**Dominikanische Republik**

DZ	**Algerien**
EC	**Ecuador**
EE	**Estland**
EG	**Ägypten**
EH	Westsahara
ER	Eritrea
ES	**Spanien**
ET	Äthiopien
EU	Europäische Union
FI	**Finnland**
FJ	Fidschi
FK	Falklandinseln (Malvinen)
FM	Mikronesien
FO	Färöer
FR	**Frankreich**
FX	Frankreich, metropolitanisch
GA	Gabon

GB	**Großbritannien**
GD	Grenada
GE	**Georgien**
GF	Französisch Guyana
GG	Guernsey
GH	Ghana
GI	Gibraltar
GL	Grönland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Äquatorialguinea
GR	**Griechenland**
GS	Südgeorgien
GT	**Guatemala**
GU	Guam
GW	Guinea-Bissau

GY	Guyana
HK	**Hongkong**
HM	Heard und die McDonaldinseln
HN	**Honduras**
HR	**Kroatien**
HT	Haiti
HU	**Ungarn**
ID	**Indonesien**
IE	**Irland**
II	International (nur Cisco)
IL	**Israel**
IM	Insel Man
IN	**Indien**
IO	Britisches Territorium im Indischen Ozean
IQ	Irak
IR	Iran
IS	**Island**

IT	**Italien**
JE	Jersey
JM	**Jamaika**
JO	**Jordanien**
JP	**Japan**
KE	Kenia
KG	Kirgistan
KH	Kambodscha
KI	Kiribati
KM	Komoren
KN	St. Kitts und Nevis
KP	KP Korea, Nordkorea
KR	**Korea, Südkorea**
KW	**Kuwait**
KY	Kaimaninseln
KZ	**Kasachstan**
LA	Laos

LB	**Libanon**
LC	St. Lucia
LI	**Liechtenstein**
LK	**Sri Lanka**
LR	Liberia
LS	Lesotho
LT	**Litauen**
LU	**Luxemburg**
LV	**Lettland**
LY	Libisch-Arabische Dschamahirija
MA	**Marokko**
MC	**Monaco**
MD	Moldawien, Republik
ME	Montenegro
MF	St. Martin
MG	Madagaskar
MH	Marshallinseln

MK	**Mazedonien**
ML	Mali
MM	Myanmar
MN	Mongolei
MO	**Macau**
MP	Nördlichen Marianen
MQ	Martinique
MR	Mauretanien
MS	Montserrat
MT	**Malta**
MU	Mauritius
MV	Malediven
MW	Malawi
MX	**Mexiko**
MY	**Malaysia**
MZ	Mosambik

NA	Kein Land ausgewählt (Spezialsituation für bestimmte Acess Points)
NC	Neukaledonien
NE	Niger
NF	Norfolkinsel
NG	Nigeria
NI	Nikaragua
NL	**Niederlande**
NO	**Norwegen**
NP	**Nepal**
NR	Nauru
NT	Neutrale Zone (transitional)
NU	Niue
NZ	**Neuseeland**
OM	**Oman**
PA	**Panama**
PE	**Peru**

PF	Französisch Polynesien
PG	**Papua-Neuguinea**
PH	**Philippinen**
PK	**Pakistan**
PL	**Polen**
PM	St. Pierre und Miquelon
PN	Pitcairn
PR	**Puerto Rico**
PS	Palästinensisches Territorium
PS	USA (öffentliche Sicherheit)
PT	**Portugal**
PW	Palau
PY	Paraguay
QA	**Katar**
RE	Réunion
RO	**Rumänien**
RS	Serbien

RU	**Russische Föderation**
RW	Ruanda
SA	**Saudi-Arabien**
SB	Solomoninseln
SC	Seychellen
SD	Sudan
SE	**Schweden**
SF	Finnland (inoffiziell)
SG	**Singapur**
SH	St. Helena
SI	**Slowenien**
SJ	Svalbard und Jan Mayen
SK	**Slowakei**
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia

SR	Surinam
ST	Sao Tome und Principe
SU	UdSSR (vormals)
SV	**El Salvador**
SY	Syrisch-Arabische Republik
SZ	Swasiland
TC	Turks- und Caicosinseln
TD	Tschad
TF	Französisches Süd-Territorium
TG	Togo
TH	**Thailand**
TJ	Tadschikistan
TK	Tokelau
TL	Timor-Leste
TM	Turkmenistan
TN	**Tunesien**
TO	Tonga

TP	Osttimor (transitional)
TR	**Türkei**
TT	**Trinidad und Tobago**
TV	Tuvalu
TW	**Taiwan**
TZ	Tansania
UA	**Ukraine**
UG	Uganda
UK	Vereinigtes Königreich (inoffiziell)
UM	Kleinere Inselbesitzungen der USA
USA	**USA**
UY	**Uruguay**
UZ	**Usbekistan**
VA	Vatikanstadt (Heiliger Stuhl)
VC	St. Vincent und die Grenadinen
VE	**Venezuela**
VG	Britische Jungferninseln

VI	Amerikanische Jungferninseln
VN	**Vietnam**
VU	Vanuatu
WF	Wallis und Futuna
WS	Samoa
YE	**Jemen**
YT	Mayotte
YU	Jugoslawien (transitional)
ZA	**Südafrika**
ZM	Sambia
ZR	Zaire (transitional)
ZW	**Simbabwe**

Index

Symbole

(...)
    Access Points-Liste
        802.11, 30
        ACL, 29
        Notizen, 31
        Sicherheit, 30
    Liste der Netzwerke
        802.11, 26
        ACL, 25
        Notizen, 26
        Sicherheit, 25
*
    Access Point, 29
    Profilname, 13, 14
    Verbinden, 42

Nummern

2,4 GHz-Band oder 5 GHz-Band aktivieren, 17
802.11d, 20
802.11-Einstellungen, 17
802.11-Einstellungen verwalten, 17, 18
802.11n-Funktionen, 36

–A–

a, 26
Access Point-Details, 32
Access Points
    802.11d-Land, 33
    ACL (Autorisierungsstatus), 22
    Detail-Bildschirm, 32
    Liste, 28
    Lokalisieren eines Access Points, 54, 58
    Ping, 46
    Verbindung mit einem Access Point herstellen, 42
ACL, 22
ACP-Dateien, 64
ACS-Dateien, 64
Ad Hoc-Gerät

Hinweis, 35
Ad hoc-Gerät
Access Points-Liste, 30
Liste der Netzwerke, 26, 29
AirCheck Manager
Aktualisieren der Software im Tester, 66
Profil, 14
Transferieren von Dateien auf einen PC, 65
Übersicht, 1
Antenne
extern, 58
intern, 57
Automatische Ausschaltung, 19
Autorisiertes Gerät, 22
Autorisierungsstatus, 22

–B–

b, 26
Balkendiagrammfarben, 21
Batterie, 6
Benutzerdefinierte Signalanpassung, 61
Benutzer-Offsets, 61

–C–

Clients, 49
CURRENT.ACP, 64

–D–

Datei speichern
Profil, 15
Testsitzung, 62
Dateien
ACP, 64
ACS, 64
löschen, 63
Profile, 14
Sitzungen, 62
Transferieren auf einen PC, 65
umbenennen, 63
XML, 64
Datum, 19
DEVICE.XML, 64

–E–

Einen Access Point oder Client lokalisieren
interne Antenne verwenden, 54
Einstellungen, 14
802.11, 17
Mindestens, 7
Standardeinstellungen wiederherstellen, 67, 83

–F–

Fluke Networks
    Kontakt, 2
    Wissensdatenbank, 1
Frequenzbänder, 17

–G–

g, 26
Gastgerät, 22
Geräte erkennen
    Client wird nicht erkannt, 54
    Clients, 49
    kein Access Point erkannt, 34
    Netzwerke bzw. Access Points, 23
Guard-Intervall, 38

–H–

Hilfe (Fluke Networks kontaktieren), 2

–K–

Kanäle
    Details zur Kanalverwendung, 40
    Frequenzbänder, 17
    Kanalverwendung, 38
    Standard, 20
    Störung
        Hinweis, 35
        Verwendungsdiagramm, 40
Kennwort
    Netzwerk, 14
    Profile, 14
Konformitätserklärung, 75
Kundendienst, 2

–L–

Land, 19
    Code von Access Points, 20
    Codes, 85
    Einstellung, 19
LEDs, 5
Leistungspegel für Übertragung, 20
Liste sortieren, 27, 51

–M–

Markiertes Gerät, 22

–N–

n, 26
n40+, n40-, 26
Nachbargerät, 22
Netzwerke

Liste, 25
Ping, 46
Sicherheitsanmeldeinformationen, 14
Verbindung mit einem Netzwerk herstellen, 42
Nicht autorisiertes Gerät, 22
Nicht hörbare Access Points ausgrauen, 18
Nicht hörbare Access Points löschen, 18
Notizen, 35
(...), 26, 31

–O–

Optionen, 68

–P–

Ping
beliebige Adresse, 46
Standardadressen, 44
Proben übertragen, 17
Probe-Request-Frames
vom Tester, 17
von Netzwerk-Clients, 49
Profil, 14
Protokoll
Bildschirm, 45
Meldungen, 79

–R–

Registrierung, 1
Reinigung, 66

–S–

Schloss-Symbole
Access Points-Bildschirm, 30, 51
Netzwerk-Bildschirm, 25
Schlüssel, 5
Schwellenwerte für Balkendiagrammfarben, 21
Sicherheitsanmeldeinformationen, 14, 42
Sicherheitsinformationen, 2, 65
Sitzungsdateien
speichern, 62
SNR, 45
SNXXXXXX.ACS, 64
Software aktualisieren, 66
Software-Update, 66
Speicher, 64
Sprache, 19
Standardeinstellungen, 83
Startbildschirm, 13
Störung
Hinweis, 35
Verwendungsdiagramm, 40
Ströme, 38

Stromversorgung
Ausschaltung nicht möglich, 67
Automatische Ausschaltung, 19
Batterie, 6

–T–

Technische Daten, 69
Transferieren von Dateien auf einen PC, 65

–U–

Unsichtbar, 26, 30, 51

–V–

Verbindung mit einem Netzwerk oder Access Point herstellen, 42
Verbindungsreichweite, 47
Virtuelle Access Points gruppieren, 18
Virtueller Access Point, 18

–W–

Wartung, 65
Weltmodus, 20
Wissensdatenbank, 1

–X–

XML-Dateien, 64

–Z–

Zeit, 19
Zeitstempel
Access Points-Liste, 29
Liste der Netzwerke, 25
Zertifizierung und Übereinstimmung, 72
Zubehör
optional, 68
Standard, 3